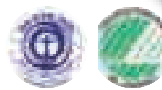
TUTTO QUELLO CHE GLI ALTRI NON DICONO



2€

NO PUBBLICITÀ
SOLO INFORMAZIONE E ARTICOLI

n. 184

www.hackerjournal.it



HACKING

IL PINGUINO SUL TOMTOM



E-MAIL

GEARS
DOP(P)IAMO GMAIL

SOCIAL NETWORK

IL GRANDE FRATELLO SI CHIAMA WAVE

TENDENZE

IL VIRTUALE FUNZIONA MALE



QUATTORD. ANNO 9 - N° 184 - 10/23 SETTEMBRE 2009 - € 2,00

FOCUS ON

STRISCIATE A RISCHIO
COME TI CLONANO IL BANCOMAT

Anno 9 – N.184
10/23 settembre 2009

Editore (sede legale):
WLF Publishing S.r.l.
Socio Unico Medi & Son S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Realizzazione editoriale
a cura di BMS Srl

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

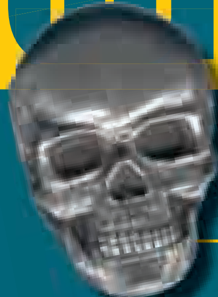
Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

hack·er (hăk'∂r)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale





Tecnologia noiosa

Dai retta a me, amico. Ogni tre lampeggi, rallenta un po'
(Fillmore in Cars)

Ogni mese escono sul mercato svariati telefonini, televisori, modelli di computer, palmari, fotocamere e quant'altro. Probabilmente le grandi aziende hanno da qualche parte migliaia di persone che pensano continuamente alla creazione di nuovi modelli dei loro prodotti: la fotocamera che integra la radio, la stessa senza radio, la stessa con il microfono stereo, il modello col microfono mono, quello senza microfono e così via, per infiniti cataloghi di prodotti sostanzialmente uguali. Dal punto di vista hacker si tratta di stupidaggini: sappiamo che non è "magico" far comunicare un ricevitore GPS con una fotocamera, sappiamo che è banale gestire 1 o 2 tracce audio, sappiamo che ogni prodotto in uscita negli ultimi anni è semplicemente composto da pezzi di tecnologie prese in prestito e assemblate. Sappiamo che è rarissimo che si inventi veramente qualcosa di nuovo, qualcosa per cui valga la pena fare carte false per avere un certo prodotto.

Da tempo, ormai, la tecnologia non sta offrendo alcuna novità reale ad esclusione della continua miniaturizzazione e sono le ricerche in altri settori a dar vita al mercato. È successo con i social network, nati da un'esigenza sociale, così come sta succedendo con i sistemi di navigazione e di car entertainment: nessuna novità, son piccoli computer in auto. Intanto la ricerca teorica, bistrattata dalle aziende perché non frutta denaro, è nelle mani di enti pubblici al collasso finanziario mentre i progetti realizzabili sembrano non avere più teorie su cui basarsi. Se continua così, ci proporranno ben presto l'acquisto di nuovissimi castelli in aria.

Intanto si avvicina la stagione calda del commercio, con l'apoteosi del Natale e le anteprime che si vedono all'orizzonte sanno di déjà vu.

The Guilty

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE
Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa!
Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Preistoria dei virus

Kaspersky Lab ha pubblicato un articolo tecnico, a cura di Magnus Kalkuhl e Marco Preuss, dal titolo "Il malware oltre Vista e XP". Ne pubblichiamo un estratto in cui si ripercorre la storia dei virus a partire dagli anni '70 quando windows significava solo "finestre".

Gli inizi turbolenti

Nei primi anni Settanta, ben prima della comparsa sulla scena di Microsoft, vi era già un virus che infettava i computer allora funzionanti con sistema operativo TENEX di DEC: il worm Creeper. Questo worm può essere ritenuto l'antesignano dei virus attuali, in quanto, per diffondersi, utilizzava ARPANET, il precursore di Internet. Creeper fu seguito da Pervade, nel 1975. Pervade, programmato per i sistemi UNIVAC, fu creato per distribuire un gioco denominato "Animal". Infine, nel 1982, fu il turno di Apple; gli utenti ebbero davvero di che "deliziarsi" con Elk Cloner, elaborato dall'allora quindicenne Rich Skrenta: tale virus si diffondeva tramite floppy disk, causando regolarmente il crollo di ogni sistema da esso infettato. Quattro anni più tardi, gli utilizzatori del C64 entrarono anch'essi a far parte del novero delle vittime dei virus informatici: il virus BHP (creato, si ritiene, dal gruppo tedesco "Bayerische Hacker Post"), in effetti, faceva sì che l'immagine visualizzata sullo schermo del computer iniziasse ad ondeggiare, ad intervalli irregolari, mentre la povera vittima veniva "salutata" con questo originale messaggio: "HALLO DICKERCHEN, DIES IST EIN ECHTER VIRUS!" (che in italiano potrebbe suonare come: "SALVE MIO BEL CICCIOTTELLO: QUESTO SI' CHE E' UN VIRUS BELL'E BUONO!"). Il testo era poi seguito da un numero di serie, il quale veniva incrementato di una singola unità ad ogni nuova infezione prodottasi. Il virus BHP, reso immune da svariati comandi di interruzione, era in grado di sopravvivere anche in caso di reset del sistema.

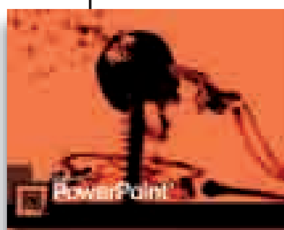
Il primo malware pet MS-DOS fece la sua comparsa nel 1986. Brain era un virus che infettava il boot sector dei dispositivi di memoria; è davvero singolare come il codice di tale malware includesse nomi, indirizzi e numeri di telefono dei suoi autori. Amjad e Basit Farooq Alvi, due fratelli di nazionalità pakistana, asserirono all'epoca di aver creato Brain per determinare a quale livello fosse il fenomeno della pirateria informatica in India. Dovettero però ammettere, in seguito, di aver perso il controllo sull'esperimento messo in atto. Negli anni seguenti, si assistette ad una vera e propria "fioritura" dei virus informatici; entrarono presto in scena virus per ogni sistema operativo allora esistente. Fu così rilevata la presenza di oltre 190 programmi malware rivolti alla piattaforma Amiga di Commodore, mentre Atari ST fu preso di mira da un altro paio di dozzine di virus. Faceva parte di questi ultimi il virus "C't" http://www.stcarchiv.de/am88/06_viren.php, così denominato in quanto pubblicato nell'anno 1988 con C't, rivista sorella di iX, in linguaggio Assembler; il virus poteva in tal modo essere copiato e riprodotto dai lettori di quel magazine di informatica. Ciò testimonia, in maniera molto evidente l'atteggiamento eccessivamente disinvolto che veniva all'epoca adottato nei confronti del malware.



La rete Arpanet così com'era strutturata agli inizi del 1974.

VENTICINQUE ANNI DI TEDIO

PowerPoint, il popolarissimo e al tempo stesso odiatissimo software per presentazioni, compie 25 anni. Nacque infatti il 14 agosto 1984 Presentation (questo il suo nome iniziale), realizzato non da Microsoft, ma dalla californiana Forethough. Nell'agosto del 1987, Microsoft comprò la Forethought per 14 milioni di dollari. Presentation fu ribattezzato PowerPoint e fu sviluppato ulteriormente da Microsoft per Windows e per Mac. Oggi ha 500 milioni di utenti che mostrano al pubblico o ai dipendenti o ai clienti circa 30 milioni di presentazioni ogni giorno e vende ogni anno per un controvalore di oltre 100 milioni di dollari, detenendo il 95% del mercato del software per presentazioni. Ma la cosa peggiore che possiamo imputare al software sono le pallosissime presentazioni di foto di bambini, animali, vignette e amenità varie che ogni giorno ci bombardano la mail.



SNOW LEOPARD GRAFFIA IL PREZZO

Un nuovo sistema operativo che incorpora applicazioni native a 64 bit, capaci cioè di gestire una maggior quantità di memoria, pur rimanendo compatibili con le versioni a 32 bit. Quindi i classici Mail, iCal, iChat e Safari saranno da subito più veloci e reattivi, così come la gestione del Finder. Un nuovo sistema che aumenta in punti di contatto con l'ambiente Microsoft e infatti incorpora il supporto nativo a Microsoft Exchange, nato per sincronizzare le reti aziendali. In un contesto in cui la sincronia tra applicazioni e piattaforme diverse in un'unica realtà aziendale è spesso un problema, l'integrazione di Exchange in ambiente Mac è certamente una mossa astuta da parte di Apple. Un sistema operativo comprensivo del nuovo OpenCL, uno standard aperto, definibile come un protocollo d'intesa tra il cuore vero e proprio del computer (la CPU) e la sua componente grafica (la GPU), la "divisione" del computer che determina la qualità di ciò che appare sullo schermo. Un protocollo da tempo vagheggiato in ambito informatico, e che Apple porta in casa degli utenti. Quali sono i vantaggi è presto detto: spesso la capacità della GPU è sottoutilizzata in ambito produttivo, mentre la CPU è facile all'affaticamento a causa del software contemporaneo, che fa spesso affidamento sulla potenza del computer piuttosto che sull'efficienza del codice con cui è realizzato. Tutto questo a un prezzo incredibile per un sistema operativo: € 29,00 spese di spedizione incluse.



YOUTUBE INIZIA A PAGARE

Google ha annunciato che intende ampliare lo YouTube Partnership Program, consentendo a un maggior numero di utenti rispetto a prima di incassare denaro tramite i propri video. Gli eletti cui verrà offerta questa possibilità saranno contattati da Google via email dopo aver verificato alcune condizioni: l'alto numero di visualizzazioni dei video, il loro propagarsi rapidamente tramite il passaparola tra utenti (la cosiddetta viralità) e la conformità alle condizioni d'uso di YouTube.

IL GRANDE PASSO DI NOKIA



Dopo tante voci è arrivata la conferma, il colosso finlandese sbarca nel mondo dei notebook e presenta il suo Nokia Booklet 3G, aggiungendosi alla lista dei produttori di telefonini già presenti in questo mercato, vedi Samsung e LG. Integrando la connettività 3G il Booklet si collega direttamente a Internet senza bisogno di chiavetta (war driving addio), il gps è ovviamente integrato e l'autonomia, vero pezzo forte, arriva a ben 12 ore: un'intera giornata di lavoro in viaggio sempre connessi! Vi ricordate la battaglia tra Mac e PC? Vera preistoria, oggi gli scenari sono ben più complessi e si giocano su vari fronti: smartphone, netbook, notebook e i colossi che gli stanno dietro. Chi vincerà? A noi poco importa, guerra commerciale significa guerra dei prezzi, per una volta l'utente finale potrebbe guadagnarci.

WINDOWS PATCH DAY

Windows non si smentisce mai: questo mese ha scelto il giorno 11 per rilasciare ben 9 patch, di cui 5 etichettate come critiche e 4 importanti. Dopo i due Patch Day di Luglio, nove aggiornamenti importanti non sono affatto male e questa volta non è Vista a fare la parte del leone, con tre miseri avvisi: Visual Studio, dopo l'aggiornamento extra di Luglio, è ancora protagonista. Analoga situazione per Office, XP e 2000, che pur non essendo (Office a parte) più in commercio rivelano ancora enormi problemi di sicurezza. Quali non è dato saperlo, visto che da Redmond, come al solito, i commenti alle patch escono solo dopo aver effettuato gli aggiornamenti.



60.000 INFEZIONI

Sono ormai più di 60.000 i siti che ScanSafe, società specializzata in sicurezza informatica, indica come colpiti da un exploit che li utilizza per installare malware sui computer dei visitatori. L'attacco ai siti avviene cercando e sfruttando una vulnerabilità di tipo Sql injection: se ha successo, quando i visitatori apriranno le pagine infette troveranno ad aspettarli un iframe che punta a un sito cinese, il quale si occuperà di eseguire uno script che scaricherà sul Pc diversi malware provenienti da sette siti differenti. Tra questi si segnalano Gologger, un trojan, diversi programmi che sottraggono le password e i dati sensibili e alcune backdoor. Molte delle vittime corrispondono a siti di istituzioni e organizzazioni più che rispettabili (per esempio il sito del New York Methodist Hospital è stato colpito): non è dunque detto che, navigando soltanto su domini conosciuti, ci si metta al riparo da ogni pericolo.

Notizia esplosiva per iPhone

Una guardia giurata francese è rimasta ferita, nello scoppio del proprio iPhone. Yassine Bouhadi, ventiseienne, stava scrivendo un SMS alla fidanzata quando lo schermo delliPhone è esploso, ferendolo a un occhio con una scheggia. Il giovane è intenzionato a sporgere denuncia.L'incidente ricorda gli altri casi emersi nelle ultime settimane: dall'iPod Touch "esploso" a Liverpool, a un altro caso in Francia, fino ad arrivare a un possibile - ma tutto da verificare - caso italiano. Ironico notare come i casi si stiano moltiplicando, aprendo la strada ad alcuni legittimi interrogativi: qualcuno sta cercando di fare il furbo per ottenere un lauto risarcimento? Oppure Apple, come fanno altre aziende, dovrebbe iniziare a prendere in considerazione il ritiro in massa dei prodotti (iPod Touch e iPhone) dal mercato? La Commissione Europea, interessata alla tutela dei consumatori, ha chiesto lumi ad Apple. La casa di Cupertino ha risposto etichettando le vicende come "casi isolati", pur confermando di essere intenzionata a capire l'origine del problema e risolverlo il prima possibile. Nuovi dettagli saranno comunicati da Apple solo al termine dell'analisi dei prodotti esplosi.



PERFIDA ALBIONE

Dopo la Francia è il turno della Gran Bretagna, chi si azzarda a scaricare riceverà il fatidico cartellino rosso: fuori da Internet.



O almeno questa sarebbe l'intenzione del governo inglese che ha addirittura dato un ulteriore giro di vite alla prima proposta che prevedeva una prima lettera di avviso a chi veniva sorpreso in attività legate al file sharig, seguita da un intervento dei provider che avrebbero dovuto operare una restrizione della banda a chi avesse perseguito nella sua attività di scarico. La nuova versione farebbe piazza pulita di ogni fase intermedia: scarichi? Ti avviso e ti taglio la banda. Questa linea dura sarebbe il frutto di un accordo tra il ministro dell'Industria Mandelson e alcuni personaggi "indipendenti" e assolutamente "disinteressati" quali i rappresentanti delle grandi compagnie cinematografiche e musicali. Varie associazioni sono già sul piede di guerra e non ci resta che aspettare e sperare che questa legge faccia la stessa fine di quella francese, rigettata in quanto ritenuta incostituzionale.

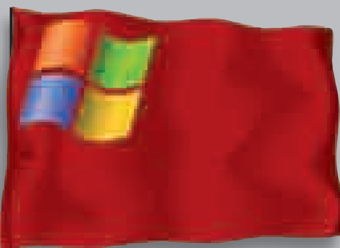
FLAGGED WIKI

Una piccola rivoluzione attende la versione di Wikipedia in lingua inglese: entro poche settimane le modifiche alle voci relative a persone viventi non saranno più pubblicate direttamente ma dovranno prima venire approvate da uno tra i volontari con maggiore esperienza.
La decisione segue i sempre più numerosi casi di "vandalismo" che interessano molte voci popolari; recentemente c'è stato il caso relativo alla morte di Michael Jackson. La pratica della flagged revision (verifica delle revisioni) non è una novità assoluta per Wikipedia: l'edizione tedesca dell'enciclopedia online l'ha adottata l'anno scorso, affidando il controllo delle voci a un esercito di 7.500 revisori. La versione in lingue inglese, tuttavia, è la prima e la più ricca tra le varie edizioni (contiene più di 3 milioni di articoli ed è consultata da circa 60 milioni di americano ogni mese) e la decisione di limitare le modifiche ad alcuni argomenti sta ottenendo una maggiore risonanza nella Rete rispetto a quanto accaduto nella sola Germania.Nel tempo Wikipedia si è evoluta e ha acquisito una certa autorevolezza: se vuole preservarla deve trovare un sistema che garantisca la correttezza delle informazioni riportate anche trasformando una delle caratteristiche che la resero così innovativa al momento del lancio.



MICROSOFT VS CINA

Microsoft festeggia la prima grande vittoria contro la pirateria cinese: due persone, Hong Lei e Sun Xiansheng, sono state condannate a tre anni e mezzo di prigione e a pagare una multa di 146.000 dollari per aver distribuito copie illegali di Windows Xp.
I due gestivano un sito, chiamato Tomato Garden ormai non più operativo, dal quale era possibile scaricare gratuitamente copie del sistema operativo di casa Microsoft Windows Xp. L'Os sarebbe stato scaricato circa 10 milioni di volte, facendo guadagnare i creatori del sito grazie alla pubblicità contenuta in esso.



IL MERCATINO DI FACEBOOK

Chi l'ha detto che facebook serve solo per incontrare vecchia mici che non vedevamo più di 20 anni (e forse c'era anche un motivo)?
Si avvicina il giorno della riapertura delle scuole ed ecco che sul social network più amato dagli italiani troviamo più di 20 gruppi che si occupano della vendita di libri usati. Il risparmio

HOT NEWS

LA MELA BACATA

Android e iPhone ancora nel centro del mirino: secondo Collin Mulliner e Charlie Miller, esperti di tecnologie per la telefonia mobile, è possibile prendere il controllo degli smartphone con sistema operativo Android sfruttando una falla macroscopica del sistema di protezione. Fantainformatica applicata al mondo hacker? Niente affatto, al Black Hat di Las Vegas hanno anche effettuato una dimostrazione pratica della loro scoperta. Con un semplice sms hanno inviato ad un iPhone uno script autoeseguibile. Non è stato necessario leggere il messaggio di testo, non appena raggiunto l'apparecchio bersaglio lo script è entrato in funzione consentendo ai due hacker di accedere alle impostazioni dello smartphone inibendo le funzioni di connettività. L'azione era mirata a sensibilizzare i produttori di smartphone che utilizzano Android (Apple in testa) del pericolo latente. Ma mentre Google e il team di sviluppatori di Android hanno risolto il problema, pare che da Cupertino tutto taccia. Anzi, nel nuovo aggiornamento del sistema operativo per iPhone (il 3.1) la risoluzione di questo bug non è stata nemmeno presa in considerazione. Potenzialmente tutti gli iPhone del mondo possono essere isolati.



PUBBLICITÀ A PICCO

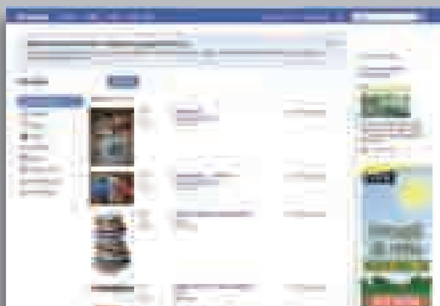
Un'indagine IDC stima per il secondo trimestre del 2009 una caduta del 5% per l'advertising online rispetto al secondo trimestre del 2008, passando da 14.7 miliardi di dollari complessivi a 13.9 miliardi. Mentre l'oriente sembra reggere l'onda d'urto della crisi (con buoni risultati soprattutto in Giappone e nell'area del Pacifico), in occidente la caduta è più pesante e negli Stati Uniti gli investimenti sono scesi del 7% nel trimestre di riferimento passando da 6.6 miliardi di dollari a 6.2. Secondo IDC la rotta non verrà invertita presto: per il prossimo semestre ci si attendono ancora spinte al ribasso, ma le percentuali dovrebbero essere minori in attesa di tornare realmente a crescere entro la metà del 2010.

JESSICA BIEL LA KILLER DEL WEB

A sostenerlo è McAfee, che evidenzia come il venti percento dei siti Web indicizzati da Google con il nome dell'attrice rimandi a link potenzialmente infettanti. In questa particolare classifica la Biel scalza Brad Pitt, che lo scorso anno vantava il medesimo primato e quest'anno si ritrova quindicesimo. I rischi maggiori di incappare in virus, spyware e altra immondizia si hanno associando al nome dell'attrice termini come screensaver, download, photos o ringtones. La Biel precede in classifica la cantante Beyoncè e Jennifer Aniston. Curioso il fatto che dalla top 15 stilata da McAfee siano assenti i coniugi Obama. I pericoli più consistenti si hanno cercando di scaricare suonerie di canzoni famose: i siti di suonerie delle canzoni di Rihanna, per esempio, pare siano i favoriti per il phishing di dati sensibili. Anche i truffatori hanno i loro gusti musicali!



è garantito, le condizioni dei libri un po' meno ma con quello che costano quelli nuovi non stiamo troppo ad andare per il sottile e almeno proviamoci.



NIENTE STREET VIEW IN SVIZZERA

Google non s'impegna a sufficienza nell'oscurare le targhe e i volti fotografati da Street View e quindi deve "togliere immediatamente il servizio da Internet": l'ingiunzione proviene da Hanspeter Thür, Incaricato federale svizzero per la protezione dei dati. Dopo le perplessità del Regno Unito, quelle della Grecia e quelle dell'intera Comunità Europea Google ora deve rispondere alle accuse elvetiche: la società ha fatto sapere di avere in programma un incontro con le autorità.



La Grande Onda

Una presentazione con i fiocchi per l'arrivo di Google Wave: promette molto, ma solleva anche molti dubbi

La notizia è di quelle ufficiali, con tanto di presentazione pubblica via YouTube e pagine Web che sembrano proprio strutturate per creare l'attesa e stuzzicare la curiosità di addetti ai lavori e non: presto avremo accesso ai servizi di Google Wave, una tecnologia studiata dagli sviluppatori della casa dalla grande G e che permette di lavorare in team attraverso la Rete in maniera semplice e intuitiva, riducendo al minimo i tempi morti di un metodo di lavoro tradizionale. Tecnicamente, si tratta di una via di mezzo tra un social network e un Office online come Google Docs, in cui i collaboratori possono lavorare contemporaneamente sugli stessi documenti proprio come si farebbe in una riunione in cui tutti intervengono personalmente, con la differenza che il proprio contributo viaggia attraverso i cavi delle strutture telematiche.

:: Più in dettaglio

La definizione che Google stessa dà di Wave (l'elemento fondamentale della sua tecnologia) è: parte conversazione, parte documento. Vale a dire, mentre parliamo con i nostri collaboratori, possiamo apportare modifiche al documento in lavorazione, fino a quando non ha la forma desiderata e, con il contributo degli intervenuti, raggiunge la struttura definitiva. Esattamente come in una riunione di team, solo che questa deve essere organizzata e comunicata per tempo, tutti devono essere fisicamente presenti e, normalmente, non è possibile lavorare tutti insieme sullo stesso documento. La tecnologia che permette invece di lavorare insieme anche da luoghi diversi, basta disporre di una connessione a Internet, è il solito Web 2.0, così come viene chiamato l'insieme di tecniche che si basano su strumenti tradizionali (come il semplicissimo Javascript) per offrire un nuovo livello di interazione con le applicazioni via Web.
Alla base di Wave c'è un nuovo protocollo di comunicazione tra client e server che Google ha denominato

Google Wave Federation Protocol. La cosa interessante è che Google ha reso le specifiche di questo protocollo completamente Open Source: ciò significa che chiunque può contribuire allo sviluppo dello stesso e delle applicazioni che lo adottano. Chi vuole maggiori informazioni su questo protocollo può visitare il sito http://www.waveprotocol.org, in cui sono descritte tutte le tecnologie necessarie ed è disponibile il codice sorgente che permette di implementarle. La struttura fondamentale si basa su messaggi XML che vengono letti dai diversi server poi rielaborati e prelevati via AJAX dai client che partecipano al Wave.



La home page del sito Internet dedicato al protocollo che sta alla base di Wave: Google Wave Federation Protocol, una piattaforma integrata che contiene praticamente tutto.

:: Per interfacciarsi

Come d'uso ormai per diverse delle tecnologie che Google mette a disposizione del pubblico, anche Google Wave si apre agli sviluppatori di tutto il mondo, non solo grazie alla presenza di un protocollo Open Source (che serve principalmente per chi vuole creare i propri strumenti basandosi sulla tecnologia), ma anche attraverso le API di Google Wave, che servono ai programmatori per interfacciarsi con gli strumenti propri del nuovo pupillo di Mountain View. All'indirizzo http://code.google.com/apis/wave troviamo tutte le specifiche, nel caso dovesse interessarci la possibilità di sviluppare gadget o nuove applicazioni per Wave. Gli elementi che si possono creare con le librerie rese disponibili da Google sono di due tipi: le estensioni, che aggiungono funzionalità a un Wave come gadget o nuovi strumenti di collaborazione e di interazione tra gli utenti, andando quindi ad arricchire ciò che Wave stesso offre di serie, o più semplicemente un oggetto Embed, che ci permette di includere un Wave nelle nostre pagine Web per fare in modo che i nostri visitatori, sia che si tratti di colleghi che lavorano in team sia navigatori che giungono sul nostro sito, possano interagire tra loro in diverse maniere. All'indirizzo http://code.google.com/intl/it/apis/wave/guide.html troviamo tutte le istruzioni che ci permettono di iniziare a sviluppare su piattaforma Wave, anche se al momento si tratta di un nuovo servizio di Google in piena fase di sviluppo e, conoscendo il produttore, mai si saprà quando si potrà parlare di versione definitiva.



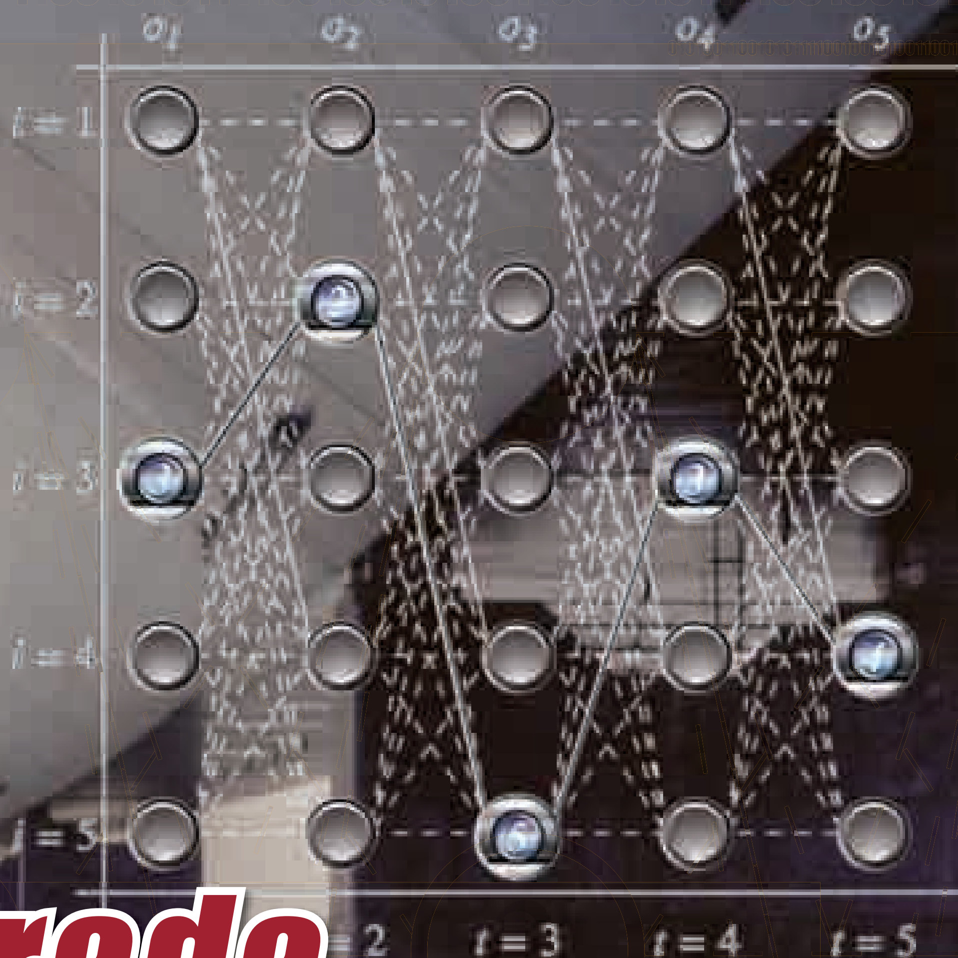
Con Google Wave i collaboratori si riuniscono sul Web per terminare un documento, in un ambiente più social network che Office.

:: Dubbi e perplessità

Non abbiamo ancora digerito del tutto i vari GMail, Docs e così via, e già Google ci propina un nuovo servizio online che non è propriamente di cloud computing ma ci si avvicina molto. La cosa ci lascia un po' perplessi, non tanto perché in questo caso non si tratti di un servizio veramente utile o perché non ne riusciamo noi a capire l'utilità, quanto per il fatto che ogni volta che sentiamo parlare di server centrali che raccolgono informazioni sugli utenti o, come in questo caso e in Docs, il loro lavoro, ci sorgono diversi dubbi che ancora non siamo riusciti a dissipare. Parliamo chiaro: server centrale significa che i nostri dati, il nostro lavoro e le nostre conversazioni non sono conservate sul nostro PC, ma su un computer esterno, e poco importa che sia marchiato Google, Microsoft o quant'altro, sempre di server esterno si tratta.

Chi avrà accesso effettivamente a quelle informazioni? Siamo certi al 100% che solo noi possiamo accedere ai nostri dati, e nessun operatore del provider del servizio mosso da morbosa curiosità ne venga attratto come una mosca dal miele? Ma soprattutto, ed è il dubbio che più di tutti ci lascia qualche remora, cosa succede ai nostri dati se quel server, o quell'insieme di server, vengono violati da malintenzionati, si guastano, vengono resettati per errore o intenzionalmente, dato che non è in alcun modo in nostro potere controllarne l'affidabilità? Ai posteri, come si suol dire, l'ardua sentenza.

Il GPS, gli OCR, il riconoscimento vocale e le trasmissioni radio spaziali hanno qualcosa in comune



La strada più breve per...

C'è un gioco in cui si ascolta una parola o una frase sussurrata in un orecchio da un compagno, cercando di capirla, per ripeterla a un altro compagno nel modo più preciso possibile. I risultati sono spesso esilaranti perché, in folti gruppi, è difficile che il passaggio a bassa voce da una persona all'altra lasci immutato il messaggio: è il classico esempio in cui si può capire "Roma per Toma". Se nel gioco, l'incomprensione può essere fonte di divertimento, nel mondo reale, specie quando si parla di tecnologia, un'incomprensione può essere catastrofica e gli esempi si sprecano: da sonde che si schiantano a esplosioni in volo, da messaggi vitali che vengono ignorati perché incomprensibili a computer che fanno le bizze.

:: Percorsi

Nel 1967, Andrew Viterbi pubblicò un articolo in cui spiegava un algoritmo concepito per migliorare la trasmissione di dati nello spazio. Viterbi è un naturalizzato americano il cui nome è tuttavia italianissimo: emigrato nel 1939 negli USA a seguito dell'emanazione delle leggi razziali, è nato a Bergamo nel 1935. Tralasciando dimostrazioni matematiche e trattamenti troppo approfonditi, comunque possibili con una banale ricerca sul Web, il concetto espresso è comunque comprensibile anche ai non addetti ai lavori: l'applicazione di un opportuno algoritmo che tenga in considerazione gli stati più probabili di un segnale, calcolati in base agli stati passati, può semplificare l'identificazione corretta del segnale trasmesso anche in condizioni di forte disturbo. Se un segnale viene ricevuto in modo poco comprensibile ma dipende dai segnali ricevuti in precedenza, l'applicazione di un algoritmo può permetterci di restringere il campo in cui cercare il segnale corretto. Di più: questo algoritmo dovrà usare come criteri di decisione la distanza minima di Hamming oppure la distanza euclidea con il segnale precedente per determinare il segnale ricevuto. Il concetto, di difficile comprensione anche se semplificato rispetto ai termini ingegneristici con cui andrebbe espresso, è più facilmente assimilabile con un esempio: immaginiamoci di dover interpretare le lettere

che compongono una parola in lingua italiana. Se in precedenza abbiamo interpretato delle lettere e hanno formato la semi-parola "lavand", l'interpretazione della lettera successiva non dovrebbe essere casuale: sappiamo che si sta usando la lingua italiana, sappiamo il contesto in cui stiamo operando e quindi possiamo assegnare una certa probabilità di comparsa ad ogni possibile lettera successiva. La lettera "a" sarà certamente più probabile ("lavanda", "lavandaia", ecc.), insieme alla lettera "i" ("lavandino") mentre la lettera "z" o la lettera "t" avranno una possibilità quasi nulla di comparire. L'algoritmo di Viterbi indica semplicemente di considerare tutte le possibilità scegliendo quella più probabile in base a una regola precisa e alla considerazione dei segnali precedenti: ad ogni passaggio vengono eliminati gli elementi più improbabili fino a ritrovarsi con un solo elemento possibile. Per questo motivo, la rappresentazione grafica dei risultati dell'algoritmo di Viterbi appare come un percorso all'interno di tutte le combinazioni possibili di elementi (**Figura 1**).

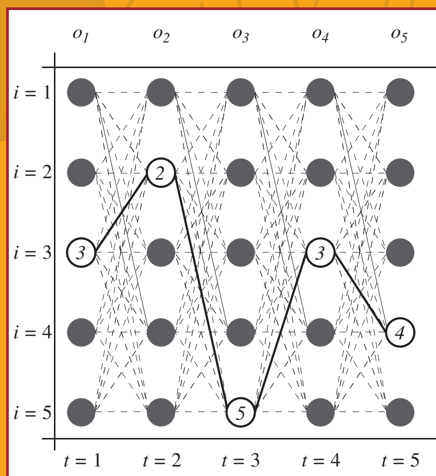


Figura1. Lo schema decisionale dell'algoritmo di Viterbi, con il tipico diagramma di ogni combinazione, detto a traliccio.

L'esempio appena fatto non è casuale perché è una delle applicazioni più conosciute di questo algoritmo: il riconoscimento dei caratteri, ottico e vocale. È proprio grazie all'introduzione dell'algoritmo di Viterbi, anche in forme spurie, che il progresso nel riconoscimento dei caratteri e della voce è stato così veloce negli ultimi anni e, detto per



Foto di Ryan K Morris/NSTMF

Andrea Viterbi con l'ex presidente Bush in occasione del ricevimento della sua medaglia per la tecnologia e l'innovazione.

inciso, questo è lo stesso motivo per cui la dettatura di testi al nostro computer offre risultati straordinari se fatta per frasi e risultati scarsi se fatta parola per parola. Nel primo caso, l'algoritmo interviene con parole intere su percorsi di possibilità molto marcati. Nella dettatura parola per parola, l'algoritmo di riconoscimento lavora sulle singole lettere, con ventagli di possibilità piuttosto ampi.

:: Cosa stai per dire?

L'algoritmo di Viterbi è una intuizione geniale che ha notevolmente precorso i tempi. Quando venne pubblicato l'articolo della sua presentazione, l'autore stesso ammetteva che non erano ancora disponibili le tecnologie necessarie per una sua applicazione pratica.



Il contributo più conosciuto di Andrew Viterbi in campo informatico è stata la fondazione di Qualcomm, creatrice di Eudora, nel lontano 1985.

Un motivo in più per cui va attribuito a Viterbi l'ulteriore merito di non aver pensato solo all'immediato ma di aver posto le basi per una serie di studi che oggi risultano piuttosto concreti. La correzione dei segnali, infatti, è sempre stata fatta usando informazioni ridondanti, codici di CRC, codifiche di vario genere. L'algoritmo di Viterbi interviene e dà un contributo determinante quando, invece, l'informazione è persino mancante. Certamente, esiste la possibilità di errore ma questa viene ridotta a un minimo nemmeno confrontabile con la casualità. Ci sono anche ambiti in cui l'algoritmo viene applicato su segnali mancanti, offrendo risultati che, ai più, appaiono miracolosi. Tra le varie applicazioni dell'Algoritmo di Viterbi nel mondo attuale ce ne sono alcune che ci vedono protagonisti tutti i giorni: senza questo algoritmo sarebbe stato impossibile lo sviluppo delle tecnologie di trasmissione e codifica digitali. Un giro di parole per dire che, senza il "rivoluzionario" Andrew Viterbi, i segnali GSM, CDMA e UMTS sarebbero rimasti nel campo della fantascienza, insieme alle mille altre applicazioni, dirette e indirette, del suo algoritmo.



CARTA CHE VINCE CARTA CHE PERDE

Il gioco delle tre carte. L'asso vince, i servizi interbancari perdono. Perché i pagamenti elettronici non sono sicuri?

In Italia la rivoluzione delle carte di pagamento è arrivata nel 1976, quando la Cassa di Risparmio di Ferrara, in via poco più che sperimentale, installa il primo sportello Bancomat. È il primo passo per la diffusione massiccia dei sistemi di pagamento basati sulla smaterializzazione fisica del denaro, almeno per come la intendiamo oggi, dove tutto è demandato all'elettronica e ai sistemi di sicurezza evoluti, o pseudo tali. Già dalla fine del 1800 si era capito come fosse necessario trovare un sistema universalmente riconosciuto per poter usufruire del proprio denaro senza averlo necessariamente con sé: assegni, Voucer di pagamento al portatore e i successivi traveller ceques sono stati gli antesignani cartacei di quello che oggi portiamo comodamente nel portafogli e che utilizziamo per effettuare qualsiasi tipo di pagamento.

:: L'illusione della sicurezza

L'idea alla base del sistema è tanto semplice quanto ovvia: non si porta in tasca denaro contante, con il duplice vantaggio di avere sempre a disposizione il proprio conto corrente con la sicurezza di non perdere nulla nel caso si venga rapinati da qualche ladrone. Solo che non è proprio così, i ladroni moderni si sono specializzati nel rubare quello che è denaro elettronico per trasformarlo in moneta sonante. Come? Le cronache dei giornali sono piene di notizie a riguardo, non passa giorno che non si senta la voce della clonazione di un bancomat o di una carta di credito. L'utente il più delle volte è tutelato, le banche sono assicurate (l'assicurazione la paghiamo nei costi di mantenimento

del conto corrente) e il maltolto viene restituito quasi in toto, ma la trafila burocratica per rimettere le cose a posto è poco agevole, e la franchigia viene persa (dai 150 ai 500 Euro in genere). Ma come funziona il sistema delle carte di pagamento elettroniche?

:: La carta

Cominciamo con il differenziare le tipologie di carte. Le due macroaree che compongono i sistemi di pagamento elettronico si dividono in carte a debito e a credito. Le carte a debito, o bancomat, sono alimentate da un conto corrente nominale, così come è nominale la carta plastica che ne identifica il possessore all'atto di un pagamento elettronico, mentre le carte di credito rispondono a un circuito parallelo e interconnesso a quello bancomat. Esistono diversi emettitori di carte di credito, che regolamentano il funzionamento della propria tipologia di carta direttamente col cliente, secondo vincoli, obblighi e opzioni di spesa differenti da carta a carta. Fisicamente, la carta è un banale supporto plastico realizzato in PVC, su cui viene impressa graficamente (utilizzando varie tecniche di stampa) logo e livrea dell'emettitore della stessa.



Nelle carte di credito è presente un ologramma con il logo della società emettitrice. Per le loro caratteristiche, queste immagini sono difficilmente replicabili senza l'uso di attrezzature molto sofisticate: se controllata, la sua presenza è una garanzia per il consumatore.

Inoltre sulla parte bassa del supporto vengono stampigliati con una stampante embossing (che effettua scritte in rilievo) nome e cognome del titolare, data di scadenza e numero identificativo della carta stessa. Il numero è parlante, ogni coppia o quaterna di cifre indica informazioni ben precise. Sul retro della carta di credito inoltre viene stampato un ulteriore codice, che dipende dalla società emettitrice della carta, denominato Credit Card Verification, più comunemente conosciuto come CCV (è quello che ci viene richiesto per i pagamenti su Internet). La sicurezza dei sistema di pagamento elettronico è data dalla carta. È la carta che identifica colui che effettua il pagamento, a tutti gli effetti viene riconosciuta come denaro contante. È per questo motivo che è la carta l'elemento del sistema soggetto al maggior numero di attacchi per impossessarsi in maniera fraudolenta del denaro. I dati che identificano la carta di pagamento, sia essa appartenente al circuito bancomat o carta di credito, sono contenuti all'interno della banda magnetica posta sul retro (secondo le nuove norme di sicurezza ABI Microcircuito saranno gradualmente sostituite con carte provviste anche di microprochip). Per utilizzare una carta è necessario disporre del Personal Identification Number (PIN), che suppone come valida l'identità dell'utilizzatore della carta stessa identificandolo come possessore. Questo vale anche per le carte di credito utilizzate in punti di pagamento automatizzati, come per esempio i distributori di benzina automatici. La banda magnetica è magnetizzata in tracce indipendenti tra di loro, normalmente quelle a disposizione per ogni carta sono quattro, di cui due (la seconda e la terza) vengono

PRELEVI? TI FREGO...



Per catturare il PIN vengono utilizzati due sistemi: il primo prevede l'impiego di una microcamera nascosta, puntata sul tastierino, che trasmette le immagini a un monitor che non può trovarsi troppo lontano dalla microcamera; nel secondo viene applicata una tastiera passante identica all'originale, che cattura i PIN e li invia al truffatore. Le microcamere sono il sistema più utilizzato, costano poco e possono essere facilmente occultate accanto alla lampada per l'illuminazione o in falsi raccoglitori delle ricevute cartacee che troviamo accanto allo sportello. Questa tecnica sta cadendo in disuso: trovare false imboccature e false tastiere è problematico e più costoso.



Una tastiera bancomat contraffatta. Identica a quella originale, cattura il codice PIN della carta bancomat e lo invia al truffatore. Spesso vengono realizzate nell'est europeo, e possono avere errori ortografici palesi. Se leggete "Anulla" probabilmente lo sportello è stato manomesso!

utilizzate per il circuito bancomat e per quello delle carte a credito. Queste ultime inoltre dispongono di un sistema di sicurezza visuale: la plastica è stampata con inchiostri fotosensibili, se viene sottoposta alla luce di una lampada di Wood (lampada a luce nera, più conosciuta come lampada a ultravioletti) appaiono i simboli identificativi della carta stessa: le lettere M e C per MasterCard, una colomba per Visa, la scritta AMEX per American Express, eccetera.

:: Il POS

Ogni dispositivo per effettuare pagamenti elettronici, normalmente chiamato POS (acronimo di Point Of Sale) dispone di un lettore di seconda e terza traccia, per poter leggere qualsiasi tipologia di carta oggi presente sul mercato. In Italia ne sono installati circa 1.300.000, presso le più svariate tipologie di esercizi commerciali: è facile capire come sia una tra le fonti regine dei tentativi di frode al sistema di pagamento elettronico. Il POS è un dispositivo dotato, oltre al lettore di banda magnetica, di un processore in grado di assolvere a molteplici funzioni, come la decrittazione dei dati contenuti in banda (o nel microchip), la ricezione del PIN del cliente, l'invio ai servizi interbancari (che si occupano di validare i pagamenti) delle transazioni elettroniche, la gestione di tutte le periferiche atte a garantire la fruizione del servizio.

:: Piccole modifiche

Il POS è il canale preferenziale per raccogliere i dati necessari a clonare una carta di credito. Dispone di tutto l'hardware necessario allo scopo: un lettore di banda magnetica, un canale trasmissivo, e un processore. Per accedervi, naturalmente, è necessario aprire le plastiche. Qui nasce il primo problema per il malintenzionato: spesso il primo sistema di sicurezza messo in campo dai produttori consiste in uno o più microswitch a pressione, normalmente chiusi, posti tra fondello e coperchio del POS. Aprendolo per manometterlo il contatto viene aperto e il software del terminale, contenuto in parte nella memoria volatile, viene perso. Il truffatore ovvia al problema identificando la posizione di questi contatti e inserendo delle lamelle prima di aprire il POS, il sistema meccanico viene così ingannato ed è possibile andare a modificare l'hardware per leggere codici e pin di qualsiasi carta venga inserita. Per la lettura della banda magnetica viene uti-

...SPENDI? TI FREGO!

Un POS è provvisto di uno o due tastierini (il tastierino alfanumerico esterno, quello che si utilizza per l'inserimento del PIN, denominato Pin Pad e quello a bordo del terminale stesso), di almeno un display, di un modem analogico o digitale (quelli con modem analogico sono ancora diffusissimi), oltre che di canali di trasmissione opzionali, quali schede di rete ethernet o moduli per la comunicazione Wi-Fi e Bluetooth. Un piccolo computer insomma, dotato di un sistema operativo proprietario, sviluppato dai vari produttori dei dispositivi stessi. Esistono diversi criteri di certificazione di un POS, il più importante si chiama EMV (attualmente di due gradi, EMV1 e EMV2), che racchiudono tutte le caratteristiche antifrode che un dispositivo deve avere per poter essere assicurato. Attenzione, non per essere sicuro, ma per far si che le compagnie rispondano in caso di clonazione di carta.

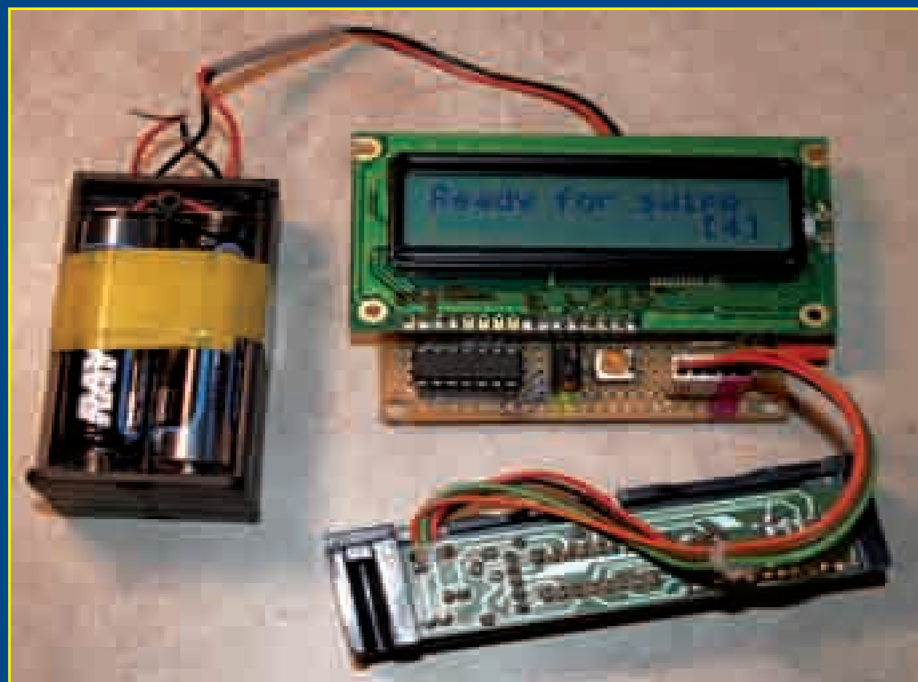


IL KIT DEL LADRO

Nel kit di un perfetto clonatore troviamo un set di cacciaviti, forbici, nastro isolante e alcuni dispositivi e apparecchiature che possono essere acquistate sul Web. Non può mancare una buona stampante per smart card, si possono trovare modelli di buona qualità a partire dai 1.500 Euro. I componenti per costruire uno skimmer fatto in casa costano molto meno, con 30 Euro si possono ottenere ottimi risultati. Discorso analogo per schede bluetooth o Wi-Fi per inviare i dati al computer: con 45 Euro se ne trovano di buoni per lo scopo. Per le carte a banda magnetica il prezzo varia a seconda delle quantità, indicativamente, per lotti di un migliaio di pezzi, costano intorno ai 90 centesimi. Una buona microcamera può costare al ladro anache 120 Euro, cifre analoghe devono essere sborsate per l'acquisto di false tastiere e false imboccature bancomat, ma non si trovano facilmente.

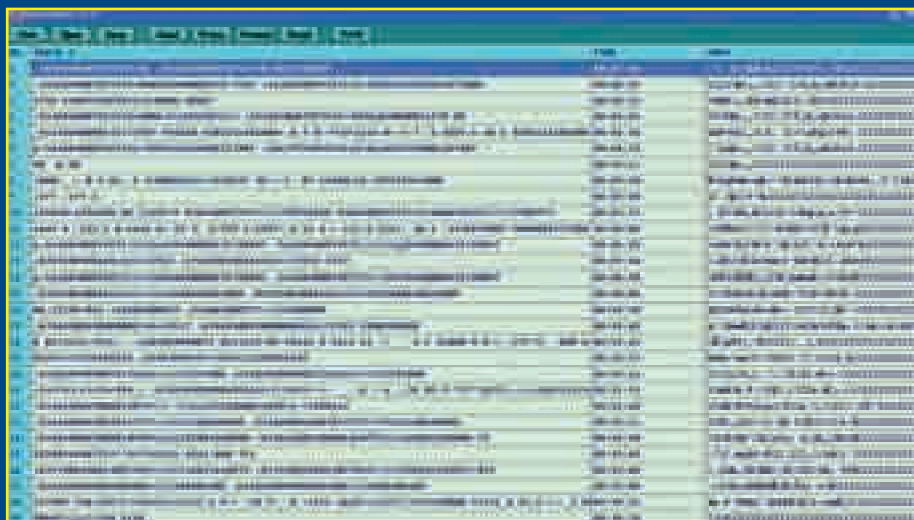


lizzato lo stesso lettore a bordo del POS: è sufficiente collegare in parallelo alla testina di lettura un processore dotato di memoria per catturare tutto quello che passa. Spesso viene utilizzato lo stesso processore a bordo del dispositivo per decodificare i dati e immagazzinarli in uno skimmer dotato di RAM. Lo skimmer è un dispositivo con un ingresso dati (il lettore di card appunto) capace di memorizzare tutto ciò che arriva dell'input e inviarlo via bluetooth o Wi-Fi a un ricevente. Alimentarlo è semplice: all'interno della scheda del POS è possibile trovare diversi punti da cui rubare tensione stabilizzata a +5 o +12 Volts, con diversi valori di amperaggio. Quindi alimentare un dispositivo esterno, qualunque esso sia, è piuttosto semplice: non c'è che l'imbarazzo della scelta. Carpiti i dati della banda magnetica, in caso di clonazione di bancomat, è sufficiente recuperare il PIN per poter replicare una carta. Per farlo viene inserita una tastiera a membrana tra la tastiera del POS e la scheda elettronica: quando l'ignaro cliente, effettuando un normale pagamento, digita su POS o Pin Pad il proprio codice segreto, questo viene catturato dalla tastiera a membrana e inviato allo skimmer. I dati vengono poi instradati al laptop o allo smartphone del cattivone via Bluetooth o Wi-Fi. Esistono delle schede in commercio già pronte all'uso, si possono acquistare per poco più di 40 dollari su Internet, in genere da siti dell'area ex Unione Sovietica. È sufficiente inserirli nel terminale di pagamento, sostituire lo stesso con l'originale all'interno del punto vendita e rimanere nei paraggi per ricevere dal POS il file di testo contenente le informazioni catturate. Una volta in possesso del clonatore, queste vengono trasferite su una carta fasulla, graficamente identica all'originale, che viene magnetizzata con uno scrittore di carte a banda magnetica.



Uno skimmer realizzato in modo artigianale, con componenti a basso costo. Una versione senza display può essere comodamente alloggiata in qualsiasi POS. Ne esistono anche di portatili: se paghiamo il ristorante con carta di credito non perdiamola di vista.

Ora la carta è spendibile, può essere utilizzata per fare acquisti e prelevamenti di contante sul territorio nazionale. L'unico modo per intercettarla è stare attenti al proprio estratto conto e segnalare pagamenti anomali al proprio istituto di credito. Gli svantaggi di utilizzare questa tecnica sono sostanzialmente due: la difficoltà di reperire un POS e, dopo averlo manomesso, di sostituirlo all'originale; inoltre bosogna essere fisicamente in prossimità del dispositivo manomesso per ricevere i dati. I vantaggi invece sono notevoli. In primis un POS ad alta affluenza, come quello di un centro commerciale, per esempio, permette di carpire i dati di molte carte in poco tempo; in secondo luogo vengono rubati sia i bancomat che le carte di credito. La carta di credito è ambita: permette spese all'estero e sul Web, per essere spesa servono solo il numero carta e il CCV.



Con un software adatto è possibile leggere, interpretare o riprodurre i dati contenuti nella seconda e terza traccia della banda magnetica di una card di pagamento.

:: ATM

È l'acronimo di Automatic Teller Machine, ma noi italiani lo conosciamo come il più tradizionale sportello bancomat. Nella classifica delle frodi è al secondo posto delle preferenze dei truffatori, perché presenta una serie di svantaggi di non poco conto: sono posti all'esterno delle banche, luoghi spesso sorvegliati da telecamere, da vigilantes o dalle forze dell'ordine; permettono di catturare perlopiù informazioni relative esclusivamente alle carte bancomat, inoltre manomettere questi dispositivi è costoso. Per la lettura della carta viene utilizzato uno skimmer posto in una falsa imboccatura carta che viene sovrapposta a quella originale, così da leggere la banda magnetica all'inserimento della card nello sportello.

COME CI FREGANO

Questi sono i sistemi maggiormente utilizzati per rubare le informazioni dalle carte di credito e dai bancomat. Per ogni segnalazione contattiamo la nostra banca e la Polizia, compilando il modulo sul sito www.poliziadistato.it.

- **Sportelli Bancomat truccati, dotati di skimmer e microcamera** Quando preleviamo verifichiamo che non ci siano microcamere nascoste e che l'imboccatura di inserimento della carta sia solida e stabile, in ogni caso quando digitiamo il PIN copriamo le dita nascondendole con la mano libera, in modo da impedire a una eventuale telecamera nascosta di rubarci il codice.
- **Terminali di pagamento POS modificati che trasmettono i dati via Wi-Fi o Bluetooth;** Verifichiamo che plastica e sigillo del POS siano integri, se il pagamento non va a buon fine facciamoci consegnare tutti gli scontrini emessi dal terminale: riporta il numero della carta di credito, che può essere utilizzato per i pagamenti sul Web.
- **Skimmer miniaturizzati, con cui leggere la carta al momento del pagamento;** Non perdiamo mai di vista la nostra carta, se siamo al ristorante non consegna mola al cameriere: potrebbe rubarci i dati leggendola con uno skimmer artigianale.

:: Contromisure

Se incappiamo in uno sportello bancomat o in un POS manomessi c'è poco da fare: cadere nella rete dei cattivi è inevitabile. Possiamo adottare degli accorgimenti che ci mettono al riparo da furti di identità telematica, ma se il lavoro è fatto a regola d'arte non c'è contromisura che tenga. Se al bancomat possiamo stare attenti, discorso diverso vale per il POS: non possiamo esaminare eventuali tracce sospette (come fori sulla plastica esterna) in un negozio, susciteremmo perlomeno ilarità. Il sistema migliore ci viene fornito ancora una volta dalla banca, che non utilizza la tecnologia a disposizione per sicurizzare i pagamenti ma ci permette di sapere in tempo reale, con il servizio sms per esempio, quando la nostra carta viene utilizzata... ha un costo, certo, ma forse è proprio per questo che la diffusione massiccia delle carte a microprocessore non ha ancora preso piede. Clonare una carta a microchip non è così semplice. Ha un file system, a cui accedere con un software dedicato. La sicurezza è demandata a un algoritmo di crittografia e per accedere al chip è necessario un protocollo. Tentare di aprire un chip significa compromettere la carta, che diventa illeggibile. La tecnologia per pagamenti sicuri c'è, ed è già vecchia, ma forse, per il modo in cui è strutturato il nostro sistema interbancario, conviene che rimanga in un cassetto.

Addio vecchia RAM



Il futuro delle amate e odiate memorie RAM è a rischio, il killer che le sta minacciando si chiama memristor

Ma cos'è un memristor? Fondamentalmente si tratta del "quarto tassello" nella trinità dei componenti passivi fondamentali della teoria dei circuiti elettrici. Secondo questa teoria ci sono tre componenti fondamentali: il resistore, che dissipa energia elettrica sottoforma di calore, il condensatore, che conserva una carica elettrica all'interno di un campo elettrico, e l'induttore, che conserva energia elettrica all'interno di un campo magnetico. Tutto questo era preso per buono finché nel 1971 Leon Chua, professore di ingegneria elettrica, teorizzò l'esistenza di un quarto elemento fondamentale, caratterizzato da una correlazione funzionale tra il flusso magnetico e la carica elettrica ai due elettrodi dell'elemento e gli diede il nome di memristor. Da allora questo componente è stato una sorta di pietra filosofale dal momento che non è stato possibile proporne un modello fisico e matematico. Solo l'anno scorso gli HP Labs hanno annunciato la realizzazione del primo modello. Il laboratorio è stato in grado di realizzare un primo esemplare reale, composto da una sottile pellicola di diossido di titanio interposta tra due elettrodi. La pellicola presenta due strati, uno dei quali caratterizzato da un leggero impoverimento di atomi di ossigeno. Le vacanze di ossigeno fungono così da portatori di carica, causando una minore resistenza nello strato "impoverito". Quando viene applicata una differenza di potenziale ai due elettrodi, le vacanze di ossigeno si spostano, variando di fatto il "confine" tra i due strati. Per questo motivo la resistenza complessiva della pellicola dipende dal "numero" di cariche che si sono spostate all'interno della pellicola di diossido di titanio in una particolare direzione. Resistenza che pertanto può variare a seconda della direzione assunta dalla corrente che fluisce nel memristor. Dal punto di vista dell'applicazione pratica, i memristor permetteranno la realizzazione di una nuova famiglia di memorie in grado di conservare informazioni anche in assenza di corrente e che potranno sostituire le odierne memorie RAM grazie alla capacità di poter istantaneamente recuperare i dati richiesti, ad esempio, al momento di ripristinare un sistema dallo stato di "sleep". Ultime notizie fuoriuscite dai laboratori si HP parlano di al massimo due anni di vita per le vecchie RAM che verranno poi sostituite da questa nuova/vecchia tecnologia che non pretende refresh continui e che assicura di aumentare fino a 6 volte la capacità di memorizzazione dei dati per pollice quadrato rispetto alle più avanzate memorie odierne.



Il primo memristor è opera dei HP Labs.

Macchine virtuali?



Siamo sicuri che la virtualizzazione, oggi tanto di moda, sia l'ideale?

Gerald Popek e Robert Goldberg, due scienziati americani, nel 1974 pubblicarono un articolo intitolato "Formal Requirements for Virtualizable Third Generation Achitectures" in cui elencavano un insieme di condizioni necessarie perché l'architettura hardware potesse supportare in modo efficiente la virtualizzazione. I tre punti chiave della loro teoria erano: equivalenza, controllo delle risorse e efficienza. Equivalenza serve per indicare che un programma funzionante in un ambiente virtualizzato deve avere un comportamento, una funzionalità e un aspetto identico allo stesso programma funzionante su una equivalente macchina reale. Per fare un esempio concreto: se il calcolo di un grafico con un certo programma richiede 30 minuti con un computer con determinate caratteristiche, dovrà richiedere 30 minuti anche con la sua versione virtuale. Il secondo punto chiave riguarda il controllo che il gestore delle macchine virtuali deve poter fare: non devono esserci risorse usate da una macchina virtuale che sfuggano al controllo del programma che la sta gestendo. Nel terzo punto, l'efficienza, i due studiosi hanno teorizzato che un buon sistema di controllo delle macchine virtuali deve intervenire il meno possibile sul funzionamento degli ambienti virtualizzati.

:: Belle parole

Almeno per quanto riguarda la virtualizzazione in ambiente x86, questo studio è stato finora inapplicato: l'equivalenza è un concetto di fantasia e l'efficienza è del tutto inesistente. Lo sa benissimo chi ha cercato di installare un gioco 3D per Windows XP in una macchina virtuale qualsiasi. Il problema nasce dal fatto che il set di istruzioni IA-32 contiene ben 17 istruzioni privilegiate che vengono eseguite a livello di ring-0 del processore: PUSHF, SIDT, PUSH, POP, STR, MOV e via dicendo. Per mantenerne il controllo e poterle eseguire a un livello separato da sé stesso, il gestore di macchine virtuali, che dovrebbe presidiare il ring-0, è costretto a intervenire prima dell'esecuzione e a cambiare lo stato di esecuzione di queste istruzioni. Su sistemi senza supporto hardware adatto, queste istruzioni vengono modificate al volo dal gestore di VMM oppure viene modificato il sistema operativo guest. Il primo caso è quello decisamente più lento ed è l'ipotesi peggiore: ogni operazione svolta dal sistema guest viene controllata e trasformata subito prima di essere eseguita. Ovviamente, le indicazioni di Popek e Goldberg sulla equivalenza dipenderanno dal modo in cui vengono tradot-





VirtualBox, prodotto da Sun, ricompila parzialmente il codice in esecuzione, on the fly, in ognuna delle sue VM per renderlo eseguibile in ambiente virtuale.

te queste funzioni ma, di certo, quelle sulla efficienza crolleranno immediatamente. Basta pensare a un ciclo di 100 passi che veda coinvolta una qualsiasi istruzione sensibile che viene sostituita, a ogni singolo passaggio, con una serie di istruzioni equivalenti. Se si interviene sul sistema guest e si cercano di eliminare queste istruzioni sensibili in via preventiva, la situazione migliora di molto ma si rischia ancora di più di intaccare l'equivalenza, senza contare che una modifica del genere non è sempre possibile: bisogna rivedere l'intero codice del sistema operativo guest e adattarlo alla VM. Per fare un esempio, questa operazione viene fatta, in modo del tutto parziale, con l'installazione delle Virtual PC Addictions in ambiente Microsoft Virtual PC ma il miglioramento di esecuzione è discutibile e, oltretutto, riservato a quei sistemi operativi per cui esistono le PC Addictions.



VMWare ESX non necessita di sistema operativo host e fornisce caratteristiche di velocità e stabilità uniche nel suo genere. Purtroppo solo hardware certificato.

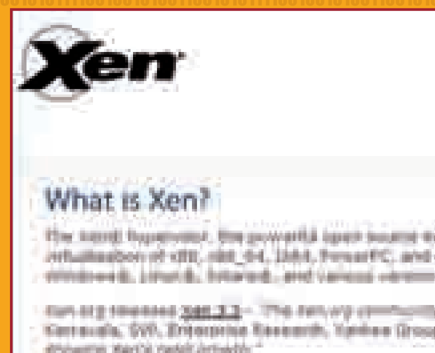
:: In garage

La strategia seguita fino a poco tempo fa era quella di minimizzare l'impatto del sistema operativo host, eliminando ogni sua funzione che non fosse dedicata alla gestione delle macchine virtuali. Da questo punto di vista, VMWare ha finora offerto la soluzione più radicale offrendo ESX, un vero e proprio sistema operativo dedicato. Microsoft ha risposto ultimamente con il suo Hyper-V, incluso in Windows Server 2008.

Il tutto è stato accelerato grazie alla novità, introdotta nelle ultime famiglie di processori con supporto alla virtualizzazione: un ring denominato -1. Una specie di seminterrato da cui si controlla tutto il resto. Creato appositamente per l'esecuzione dei gestori di macchine virtuali e a questi riservato. Lo scopo del gioco è quello di permettere ai nuovi software di virtualizzazione di far funzionare macchine virtuali senza perderne il controllo e senza sostituire le istruzioni che andrebbero allo stesso livello del manager. Il meccanismo funziona ed è ben sperimentato: i sistemi operativi non sono realizzati per girare a livelli inferiori allo 0 che, in passato, era definito come il livello dai maggiori privilegi. Così, il funzionamento in ambienti virtualizzati con il necessario supporto del processore è perfetto e, finalmente, le indicazioni di Popek e Goldberg vengono rispettate in pieno.

:: Un danno?

Questa evoluzione, sulla carta, dovrebbe essere la benvenuta ma diverse considerazioni negative vengono volutamente trascurate dai produttori a favore della pubblicità sempre più pressante sulla necessità di "consolidare i sistemi". La prima riflessione, comune a tutti gli specialisti di hardware, è che tutti questi nuovi processori non sono altro che macchine specializzate nell'emulazione e risultano certamente più costose dei loro corrispondenti privi di queste funzionalità. Non che questo sia per forza un danno ma, dati alla mano, non si vede perché investire in una macchina che costa 100 euro e destinata a sostituirne due che ne costano 40 l'una. L'unico motivo sembra essere che i produttori non vendono o non supportano più le macchine da 40 euro e, stranamente, spingono moltissimo per l'acquisto di macchine da 100. La seconda riflessione riguarda i sistemi operativi: se ne possono avviare a piacere sul proprio hardware e ognuno è allo stesso livello, non esiste un sistema host quindi non ha senso ha scegliere un sistema operativo primario. L'ultima questione è la più delicata: che sistemi di protezione esistono per quel ring -1 tanto importante? Attualmente nessuno ne parla con la sicurezza, falsa, che ogni infezione da virus possa essere distrutta spegnendo una VM. C'è da scommetterci che ci sono già persone all'opera per creare il primo virus capace di sfruttare questa caratteristica. Poi arriverà il primo antivirus capace di sconfiggerlo e c'è già chi teme, alla fine, la nascita di un ring -2 e di una serie di successivi ring il cui unico risultato sarà quello di permetterci di navigare su Internet e consultare la posta elettronica con macchine virtuali una dentro l'altra e hardware inutilmente costosi.



Xen è lo standard open source di virtualizzazione. Come molti suoi concorrenti, analizza e ricompila il codice guest. Una soluzione brillante ma non performante.



Virtual PC di Microsoft ha un dispositivo primario di analisi e ricompilazione del codice in esecuzione nella VM ma può barare se si installano le VM Addictions.

Caro Parlamento...

Un viaggio nell'Italia della precarietà lavorativa che ha raggiunto le massime cariche dello Stato

Per fortuna, la realtà in cui viviamo è molto più complessa dei luoghi comuni e delle frasi fatte che assimilano le promesse politiche a quelle da marinaio, tanto per citare un detto popolare. Per fortuna perché c'è ancora chi ha a cuore la vita politica del nostro Paese e chi se ne interessa non tanto in termini di "chi vince e chi perde", ma più semplicemente prendendo atto di quali siano le effettive necessità che gli Italiani sentono e del perché spesso il nostro ambiente politico sia troppo spesso ottuso al punto di non rendersene conto o di prenderle in considerazione solo quando conviene, per motivi elettorali o quant'altro. Da questo interessamento è nato un ottimo lavoro che sa molto di reality cracking e che, anche se non è ancora così diffuso da riuscire a raggiungere tutti noi, se non altro è riuscito ad approdare sulle scrivanie delle più alte cariche politiche dello Stato, come una sorta di messaggio nella bottiglia da parte di noi Italiani. Si tratta di un documentario, diretto da Giacomo Faenza e realizzato con l'importante contributo del Ministero per i Beni e le Attività Culturali - Direzione Generale per il Cinema, che fotografa il sentimento di quasi 200 lavoratori italiani, provenienti da tutte le Regioni e da moltisime categorie di attività, intervistati singolarmente. La cosa interessante non è solamente il fatto che esista un chiaro messaggio diretto al mondo politico, un sentimento comune di molti tra gli intervistati. Si parla anche di pecche, se proprio di pecche si può parlare, stanno anche da questa parte della linea di separazione. È una fotografia, sia chiaro, una sorta di presa d'atto: non ci sono né critiche indirizzate verso qualcuno in particolare, né men che meno accuse di alcun tipo. Comunque ciò che ne emerge è davvero interessante.

:: Punti di vista

Il campione degli intervistati spazia geograficamente da nord a sud su tutto il territorio nazionale e com-

prende persone tra i 20 e i 40, anni di tutte le estrazioni sociali e di diverse categorie lavorative. Il problema più pressante, un po' per tutti, è la precarietà che si è venuta a creare nel nostro Paese con le scelte dei governanti negli ultimi anni: precarietà dal punto di vista del lavoratore, che non riesce più a fare progetti nel tempo perché non esiste più la certezza del posto di lavoro e, quindi, di quella continuità della sicurezza economica che purtroppo è sempre alla base di tutto. Flessibilità, invece, per chi ci governa, per creare maggiori opportunità sia per i lavoratori sia per le aziende, in cui è il merito personale che prevale e che offre maggiori garanzie al lavoratore ed evita ai datori di lavoro quel senso di oppressione e di obbligo che nasce nel momento in cui un rapporto lavorativo diventa troppo vincolante. Sono due facce della stessa medaglia, a ben vedere, filtrate certo dal punto di vista dato dalla propria posizione nel sistema. E questo senza andare a mettere il dito nella piaga delle retribuzioni, perché in questo caso sì che si ricadrebbe di nuovo nel calderone delle frasi fatte.

:: Articolo 1

Parliamo della Costituzione della Repubblica Italiana. Sappiamo che c'è, la sentiamo citare spesso e soprattutto durante le celebrazioni del 25 aprile, ma quanti di noi la conoscono veramente? Purtroppo, e questo emerge a gran voce dal lavoro di Faenza, molto pochi. Pochi sanno che è la Carta che riporta per filo e per segno i diritti e i doveri di tutti i cittadini, ma anche quelli dello Stato stesso. E anche chi sa di cosa si tratta, spesso non ha chiare idee su quali siano questi doveri e questi diritti, perché ci si limita a leggerla a scuola quando necessario, ma come tanti altri argomenti entra da una parte ed esce dall'altra. Eppure, il primo articolo della nostra Costituzione cita: "L'Italia è una Repubblica democratica,



La Costituzione della Repubblica Italiana: è un bene di tutti. Quanti la conoscono e ne capiscono il profondo significato?

fondata sul lavoro". Democratica, costituita quindi dal popolo stesso, e fondata sul lavoro del popolo stesso. Bella roba, qualcuno dirà: mica ce l'hanno tutti un lavoro, soprattutto stabile. È vero: se manca il lavoro, manca anche la base stessa su cui è fondata la nostra Repubblica. Significa in sostanza che la democrazia è a rischio. Senza lavoro e senza democrazia, che popolo saremo tra una generazione? Esisteremo ancora? Ma, se proseguiamo con la lettura, troviamo che l'Articolo 4 comunica che "La Repubblica riconosce a tutti i cittadini il diritto al lavoro e promuove le condizioni che rendano effettivo questo diritto". Non lo sapevamo: il diritto al lavoro è uno di quei diritti imprescindibili che ci viene garantito non da un decreto qualsiasi, ma da un articolo della nostra Costituzione. Articolo 3, Comma II: "È compito della Repubblica rimuovere gli ostacoli di ordine economico e sociale, che, limitando di fatto la libertà e l'eguaglianza dei cittadini, impediscono il pieno sviluppo della persona umana e l'effettiva partecipazione di tutti i lavoratori all'organizzazione politica, economica e sociale del Paese". Articolo 4, Comma II: "Ogni cittadino ha il dovere di svolgere, secondo le proprie possibilità e la propria scelta, un'attività o una funzione che concorra al progresso materiale o spirituale della società". Questo significa che tutti noi abbiamo il dovere di essere cittadini vigili e con la testa sulle spalle. E se siamo disoccupati e senza futuro, dobbiamo trovare il modo di farlo capire alle istituzioni. Per esempio con un documentario, o con un articolo come questo... Gli strumenti per migliorare, quindi, li abbiamo: solo che non lo sappiamo, e non li conosciamo.

GIACOMO FAENZA

Coetaneo, amico di adolescenza e compagno di squadra (baseball), Giacomo per me è stata una di quelle amicizie con cui si riallacciano i contatti dopo molto tempo grazie alla Rete. È grazie alla Rete che sono venuto a conoscenza del suo lavoro di cui parliamo in queste pagine, lavoro che mi ha molto colpito perché mentre l'attenzione di tutti era rivolta alle notti brave dei nostri governanti, ho trovato finalmente qualcuno che riporta la politica al nostro livello, un livello più pratico, quello dei comuni cittadini. L'indirizzo del suo blog è http://caro-parlamento.blogspot.com e vale la pena seguirlo, per avere notizie su proiezioni e trasmissioni del documentario.



UN TOMTOM APERTO

È ormai una certezza: alla base del navigatore più famoso c'è Linux

Si collega facilmente a Windows e OSX, ha un'interfaccia intuitiva che ne ha fatto la fortuna, è venduto persino nei supermercati e sembra un concentrato di tecnologia incredibile: TomTom è ormai sinonimo di navigazione GPS per auto e moto. Non molti sanno, tuttavia, che il cuore di questo prodigio tecnico non è qualche sistema proprietario ma tutto è basato su Linux. Basta un'occhiata alla licenza che accompagna ogni modello, reperibile sul web all'indirizzo www.tomtom.com/page.php?Page=gpl, per accorgersi che più che un prodigio di tecnologia abbiamo a che fare con un prodotto che, con l'esclusione di alcune parti proprietarie, è persino replicabile. Un insieme di tecnologie Open Source di cui gli utenti non vedono che l'interfaccia proprietaria ma che nasconde un cuore Open.

:: Elenco infinito

Così ecco che, obbligati dai termini della licenza GPL, il team della TomTom International ci svela che i tool di sviluppo usati per compilare i programmi per l'ARM che fa funzionare l'aggeggio vanno dalle GNU binutils a Termcap, passando da un'immancabile glibc e dai font di freetype. Non solo: sempre a causa della licenza, i programmatori sono stati costretti a svelarci che il kernel stesso del dispositivo non è altro che una versione rivista e corretta di Linux la cui versione per TomTom Go si può scaricare da www.tomtom.com/gpl/golinux-tt164445.tar.bz2. Come se non bastasse, i vari modelli di TomTom includono molto altro software Open: dalle librerie BlueZ a BusyBox, da dosfstools (per leggere le FAT) a blueserver (per gestire il bluetooth). Ovvio che, con queste premesse, l'attenzione degli sviluppatori Open possa essere ai massimi storici: l'hardware dei vari modelli TomTom è di discreta qualità, le ipotesi di espansione software vanno ben al di là della navigazione e l'idea di usare i vari TomTom come piattaforme di sviluppo per programmi realizzati da indipendenti fa certamente gola. Senza contare che proprio gli utenti Linux sono attual-







Aprire un TomTom non è complicato ma invalida la garanzia. Viceversa ci permette di indagare sull'hardware al suo interno: estremamente compatto e piuttosto sofisticato.

mente gli svantaggiati dalla politica della TomTom: aggiornamenti solo per Mac OSx e Windows. I maligni dicono che i motivi stanno nel fatto che un'apertura ai sistemi Linux svelerebbe la possibilità di personalizzare troppo TomTom… Intanto, però, alcuni si sono cimentati con la programmazione sulla "nuova" piattaforma e i risultati sono stati notevoli, anche senza arrivare a stravolgere il software proprietario. Una volta scoperte le informazioni essenziali del kernel, infatti, è bastato indagare sulle configurazioni interne per capire come integrare nuovi programmi con l'interfaccia attuale ed arrivare a poter mettere le mani sul funzionamento del sistema. Oggi, grazie a questi studi, è possibile fare un po' di tutto: dall'interazione con il bluetooth tramite linea di comando o interfaccia grafica fino alla creazione di applicazioni che tengono un diario della posizione dell'apparecchio fino alla modifica automatizzata del sistema di mappatura che sostituisce le costose mappe proposte dalla TomTom con quelle di

STRUMENTI UTILI

Se ci interessa programmare sulla "piattaforma" TomTom, ci sono alcuni riferimenti indispensabili da consultare per comprendere il modo in cui pilotare l'hardware a disposizione e interagire con gli utenti. Grazie agli esempi riportati avremo una base da cui partire per la programmazione e nuovi spunti per creare utility su misura.

- **code.tomtom.free.fr**
  È un sito di base, in lingua francese, che riporta frammenti di codice, esempi e indicazioni sulla programmazione in C adattata alla piattaforma TomTom. Completo e semplice da capire, anche per i programmatori meno esperti.
- **ghotidigital.sourceforge.net**
  Una versione alternativa del classico Hello World nonché tra i primi programmi realizzati dagli utenti per TomTom. In tedesco.
- **www.opentom.org**
  Una specie di enciclopedia di tutto quello che è stato finora prodotto con gli esperimenti della comunità di utenti TomTom. Ricchissimo di codice da studiare e di soluzioni a quasi tutti i problemi che ci si possono presentare.
- **www.tomtom.com/page.php?Page=gpl**
  La pagina del sito della TomTom con l'elenco delle licenze GPL che riguardano i suoi prodotti. Un ottimo punto di partenza per capire come interagire con il software già disponibile all'interno della nostra piattaforma.

Google, ideale se si ha una connessione semi-flat a Internet. Mancano all'appello ancora software che potrebbero essere utili, come un sistema di localizzazione e antifurto (i TomTom sono tra gli apparecchi elettronici più rubati) ma la strada è ormai segnata: i TomTom vanno ormai inseriti tra le piattaforme di sviluppo disponibili.

:: Ciao!

Il metodo migliore per avere un'idea della semplicità di integrazione di un programma con TomTom è senz'altro quello di creare il classico "Hello -world!" e vedere come agisce sul dispositivo. Il linguaggio di programmazione scelto è il C e non è un caso: è ottimo per il processore ARM che equipaggia la nostra piattaforma. Per prima cosa creiamo una directory chiamata "ciao" e al suo interno mettiamo un file "ciao.c" da editare, rigorosamente, con un editor di soli testi. Ora scriviamo in C il nostro programma (**Codice 1**). Ora compiliamo l'applicazione con gcc, dando il comando "gcc ciao.c-o ciao" oppure usando il make. A questo punto dobbiamo trasferire il programma sul TomTom: basta collegarlo al computer in modalità disco. Creiamo una directory chiamata "catapps" e copiamoci il programma "ciao" compilato.
A questo punto dobbiamo integrare il programma con l'interfaccia del TomTom. Creiamo la directory SDKRegistry e inseriamo un'immagine "ciao.bmp" che verrà usata come icona dell'applicazione. Poi creiamo un file di testo chiamato "ciao.cap", da inserire nella stessa directory, in cui scriveremo le istruzioni di integrazione per l'ambiente proprietario TomTom (**Codice 2**). A questo punto basta riavviare il TomTom per trovarsi l'icona "ciao.bmp" nel menu e poter lanciare la nostra applicazione.

[Codice 1]

```
#include <stdio.h>
#include <stdlib.h>
main(void){
        FILE *out;
        out=fopen("/mnt/sdcard/loghello.txt","w");
        fprintf(out,"Hello\n");
        fclose(out);
}
```

[Codice 2]

```
Version|100|
AppName|ciao|
AppPath|/mnt/sdcard/catapps/|
AppIconFile|ciao.bmp|
AppMainTitle|ciao|
AppPort|2008|
COMMAND|CMD|ciao|ciao.bmp|Ciao|
```

::Una base, tanti usi

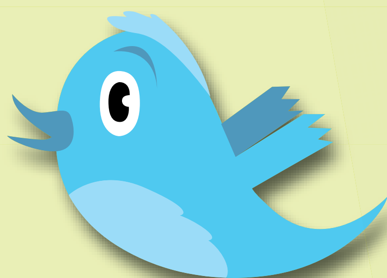
Da questa semplice base è possibile arrivare a sfruttare le diverse caratteristiche del TomTom per poter eseguire ogni genere di applicazione: grazie all'uso di una base open, la semplice consultazione dei termini di licenza ci permette di avere gli strumenti necessari a qualsiasi interazione, anche con dispositivi apparentemente complessi. Il touchscreen, per esempio, è visto dal sistema come una normale periferica che nel linux del TomTom è vista come /dev/ts. Il controllo del touchscreen, quindi, prevederà l'apertura della connessione con questa periferica virtualizzata con una sintassi del comando open di C: open("/dev/ts"). Diversi utenti di TomTom, per esempio, hanno iniziato da qui per arrivare a creare prodotti di ogni tipo che puntano a coprire alcune mancanze tipice del software proprietario del dispositivo. All'indirizzo www.webazar.org/tomtom/tripmaster.php, per esempio, si può scaricare Tripmaster, un plugin realizzato per aiutare tutti quelli che amano affrontare percorsi al di fuori delle strade tradizionali, campo in cui il classico software TomTom è estremamente carente. Se preferiamo l'utilizzo del TomTom come un tradizionale computer, invece, avremo bisogno di una console di comando. Ce n'è una, ottima, disponibile già pronta all'indirizzo www.opentom.org/TomTom_Console.
Naturalmente, tutto quanto detto finora è in continua evoluzione: malgrado l'uso di librerie basate su versioni open, alla TomTom hanno personalizzato molto il loro Linux e ci sono cose che sono tutt'ora oggetto di studio da parte degli appassionati. Un esempio riguarda le librerie grafiche: la gestione oggi possibile del TomTom è molto basilare e in molti stanno cercando il modo di sfruttare le librerie già disponibili per ottenere rappresentazioni grafiche migliori e, magari, sviluppare giochi complessi. Un motivo in più per i possessori di prodotti TomTom per abbandonare il vano inseguimento all'ultima versione delle mappe in favore di un uso alternativo e migliore della tecnologia.



Direzione, altitudine e altre informazioni utili: l'hardware TomTom è ideale per orientarsi ma le mappe non sono molto utili nei sentieri...

DDOS e il social va giù







Giù come un ferro da stiro in piscina: basta un attacco ddos per far sparire Twitter e Facebook dalla faccia della Terra

Fino a poco tempo fa, Cyxymu era solo il nome di una tranquilla cittadina della Georgia. Oggi, invece, è un nome conosciuto e temuto da tutti i gestori di siti Web del mondo a causa dell'attacco a un blogger che da quella cittadina ha preso il nickname. Cyxymu è un georgiano di 34 anni, un critico attivista del movimento contro la Russia e accanito blogger: tramite diverse piattaforme è tra i maggiori contributori delle critiche al regime di Mosca e alla politica che adotta nel Caucaso. La sua, quindi, è una battaglia strettamente condotta sul piano della parola, attraverso le opportunità offerte dal cosiddetto Web 2.0. Sarebbe una situazione normale, quindi, se non fosse che il 6 agosto, un gruppo di hacker russi ha deciso di zittirlo. Anche questo è abbastanza normale: in tempi di guerre elettroniche, in cui tutto è giocato tramite la grande Rete, è lecito aspettarsi reazioni in grande stile e con gli stessi mezzi da parte di chi viene attaccato. Particolare, però, è stato il metodo con cui questa reazione è stata condotta: non potendolo raggiungere fisicamente, non potendo agire sui server che lo ospitano, il gruppo di hacker, ufficialmente senza supporto da parte del governo russo, ha dato vita a un attacco Distribuited Denial of Service contro i siti incriminati. Per chi non lo sapesse, questo attacco non è altro che una grande quantità di richieste provenienti da moltissimi computer e dirette a singoli server. Il server che le riceve inizia a soddisfarle ma non riesce a smaltire le code di pacchetti, fino a esaurire le sue risorse e a far "cadere" un servizio. Nel caso in questione, tra i siti colpiti c'erano Facebook e Twitter e i risultati sono stati immediati: l'attacco DDos si è sommato al già elevato traffico giornaliero fino a creare disservizi su scala planetaria. Twitter ha ceduto per primo, svelando la scarsità di sistemi di sicurezza disponibili, mentre Facebook è rimasto in piedi in alcune sue parti, offrendo un servizio solo parziale e soggetto a continui errori e timeout.

:: Pericolo?

Se il problema fosse stato limitato all'attacco, sarebbe stato comunque limitato. Anche un attacco protratto nel tempo può richiedere molte risorse per poter essere arginato. Alcuni dubbi, invece, sorgono legittimamente in seguito. Dopo giorni dall'inizio dell'attacco, i siti in questione non sono ancora in grado di garantire un servizio continuativo. Mentre Facebook risente marginalmente della cosa e i suoi disservizi sono rientrati nella normalità di un sito che vede picchi di accessi su server sotto dimensionati, Twitter è tutt'ora a rischio e nessuno sa quando potrà garantire un uptime continuativo. Un fatto grave se si considera che Twitter è l'unica fonte di informazioni sulla crisi in Iran ma anche su tutto quel sottofondo di "voci" che le agenzie di stampa ufficiali evitano di riportare. C'è ancora molta strada da fare per garantire la libertà di parola sul Web se si pensa che l'attacco a un solo utente ne ha messi a tacere milioni.

DEFCON 17

Tutto ciò che ha caratterizzato l'edizione 2009

Mentre molti di noi erano già in vacanza, si è tenuta la diciassettesima edizione di DEFCON, la ormai famigerata hacker convention che ogni anno raccoglie adesioni di hacker da tutto il mondo che, oltre a scambiarsi informazioni su argomenti che riguardano la sicurezza informatica e delle nuove tecnologie, si divertono a sfidarsi in veri e propri tornei hacker, il più celebre dei quali è il classicissimo Capture the Flag. Tra numerosi interventi, eventi più o meno goliardici (siamo hacker, ci piace divertirci!) e gare di abilità di vario genere, chi ancora non ha visitato gli Stati Uniti ed è curioso di cosa significhi partecipare a una conferenza hacker farebbe bene a tener d'occhio il sito ufficiale della manifestazione (www.defcon.org) e trovarsi in quel di Las Vegas per l'edizione dell'anno prossimo.

:: Capture the Flag

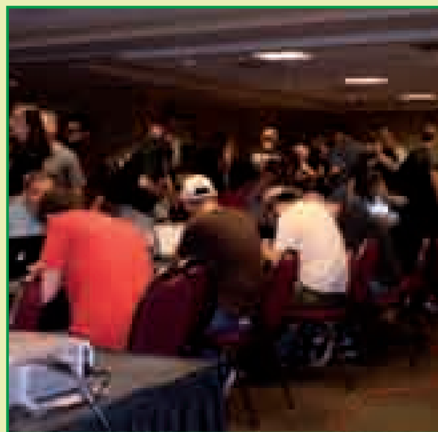
Come al solito, Capture the Flag è stata la gara tra gruppi hacker che più di tutte ha attirato l'attenzione dei partecipanti e degli intervenuti. Come avevamo accennato diversi numeri fa di HJ, gli organizzatori di DEFCON cercavano una nuova figura che si occupasse dell'organizzazione del contest e in questa edizione se ne è occupata Diutinus Defense Technologies, un'azienda che opera nel campo della sicurezza, che è stata all'altezza del compito e delle aspettative di tutti. Dopo la prima necessaria scrematura, i turni preliminari che si sono svolti nelle settimane precedenti l'evento vero e proprio, i nomi dei gruppi che sono riusciti ad accedere alla fase finale sono i seguenti: sk3wlm4st3r, Team Awesome (aka VedaGodz), Sexy Pwndas, PLUS, Shellphish, Song of Freedom, lollerskaterz dropping from roflcopters, Underminers, Routards, WOWHACKER, Sapheads_, sutegoma, CLiP, pebkac, ACMEPharm. Compli-

menti a tutti non solo per essere riusciti ad accedere al contest, ma anche per la fantasia nella scelta dei nomi... I dettagli di come si è svolta la gara li troviamo tutti sul sito di DEFCON e sul forum, ma per i più curiosi ecco la classifica finale:

1. **VedaGodz;**
2. **Routards;**
3. **PLUS@postech;**
4. **Shellphish;**
5. **Sexy Pwndas;**
6. **Song of Freedom,**
7. **Sapheads;**
8. **lollerskaterz dropping from roflcopters;**
9. **WOWHACKER.**

:: Hack the Badge

Anche se CTF rimane il contest che più di tutti attira l'attenzione del pubblico hacker, quest'anno ha avuto ottimi risultati anche Hack the Badge. Si tratta di un contest parallelo, in cui i partecipanti devono hackerare il badge della manifestazione (si tratta di una basetta elettronica aperta allo sviluppo e contenente un microcontroller con un suo programma base). Tutti i dettagli del badge di quest'anno (schemi, basette e quant'altro) si trovano all'indirizzo www.grandideastudio.com/portfolio/defcon-17-badge/. Gli organizzatori di DEFCON si sono detti meravigliati per quanto siano riusciti a fare con così poco i colleghi hacker. Senza togliere gli onori a chi non è riuscito a vincere ma ha comunque partecipato degnamente, il vincitore (Zoz) ha creato un sistema anti-sorveglianza che inibisce il riconoscimento automatico del volto da parte delle telecamere di sicurezza collegate ai PC, proiettando sul volto stesso lampi casuali di luce colorata a una frequenza inferiore ai 60 Hz per creare rumore ottico e confondere in questo modo i dispositivi di sicurezza.



La sala messa a disposizione dal Riviera Hotel & Casinò di Las Vegas.

Parte del contest prevedeva anche la realizzazione di lavori che coinvolgessero il badge dell'edizione precedente: interessante il lavoro di Team Bash Fork Bomb :(){:|:&};: che ha creato un server Web alimentato a batteria il cui sito risiede su scheda SD.

:: Gli interventi

Al di là dell'aspetto competitivo e goliardico della manifestazione, bisogna anche tenere presente che durante DEFCON numerosi speaker si susseguono per parlare al pubblico di sicurezza, nelle sue più variegate sfaccettature. Quelli che presentiamo qui sono solo alcuni degli argomenti trattati, dato che gli interventi sono stati numerosi e tutti interessanti.

Jabra e RSnake hanno parlato di problemi di sicurezza che riguardano quelle tecnologie che dovrebbero garantire la propria privacy durante gli accessi a Internet. Non soltanto i classici server proxy, ma anche altre tecnologie di questo tipo sono affette da errori di implementazione e da bachi che ne compromettono l'efficacia.

Sohail Ahmad e Prabhash Dhyani hanno dimostrato che accedendo a un area WiFi aperta e pubblica, come negli aeroporti e altri luoghi simili, siamo tutti soggetti a un attacco che mira a ricavare dal nostro portatile informazioni sulle reti wireless cui si è collegato e quindi fornisce al malintenzionato di turno gli strumenti per accedervi a sua volta. Anche le reti WPA/WPA2 non sono immuni da questo tipo di attacco. **Chema Alonso e Palako** hanno dimostrato che i documenti di



La home page del sito www.defcon.org, che ospita il programma del meeting.

Office, i file PDF e altri documenti simili che decidiamo di porre a disposizione del pubblico sul Web possono contenere numerose informazioni spurie che offrono ai malintenzionati importati dettagli su come è composta la nostra rete anche se queste informazioni non vengono visualizzate. L'esempio portato è quello dell'ex Primo Ministro inglese Tony Blair, che è stato smascherato per aver modificato un importante documento di Word proprio per mezzo di queste informazioni spurie che il programma lascia come traccia nel file.

Iftach Ian Amit ha riportato la propria esperienza vissuta durante lo studio di un server su cui girava software pericoloso messo in linea da criminali, arrivando ad avere accesso a detto server nello stesso momento in cui il criminale vi era loggato (si parla addirittura di McColo). Interessante anche l'intervento di **Myrcurial e di Tiffany Rad**, che hanno posto l'attenzione su quali sono i nostri diritti legali quando si entra nel campo della sicurezza informatica, un ambiente in cui probabilmente nessuno di noi riesce a muoversi con disinvoltura e che è comunque più che mai nell'attenzione di tutti, oggi come oggi, nel momento in cui si parla di veri o presunti Grandi Fratelli informatici e di sicurezza dei dati personali.

Alla prossima edizione!

Select * from Gmail

La casella di posta come un database



Forse non tutti sanno che, dall'inizio di quest'anno, Gmail consente di creare una versione locale della propria casella di posta, accessibile anche quando si è offline. Tramite l'utilizzo di Gears, un'applicazione di Google che si installa come estensione del browser, è infatti possibile creare applicazioni Web che funzionano anche quando il PC è scollegato da Internet. Non potendo resistere alla curiosità, abbiamo controllato dove e in quale formato viene salvata la posta sui nostri dischi, scoprendo alcune informazioni interessanti...

:: Installiamo Gears

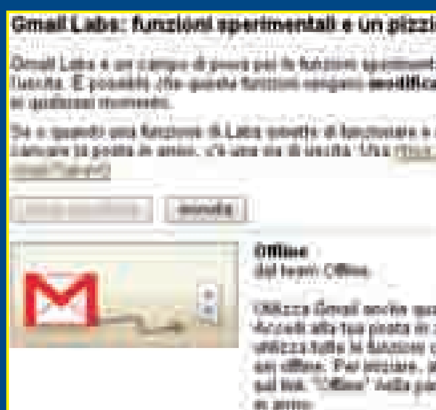
Gears è disponibile per Windows (con Firefox o Internet Explorer), Windows Mobile (con IE Mobile o Opera Mobile), Mac (Firefox e Safari), Linux (Firefox) e Android. L'installazione di Gears è molto semplice: è sufficiente infatti collegarsi all'indirizzo http://gears.google.com, selezionare l'opzione "Install Gears" e accettare i termini del contratto per scaricare l'estensione del browser desiderata. Una volta installata l'applicazione, è sufficiente riavviare il browser per renderla attiva.

:: Scarichiamo la posta

Grazie a Gears possiamo effettuare il download della nostra casella di posta in modo che sia disponibile offline: per fare questo ci colleghiamo a Gmail e selezioniamo l'opzione "Offline" dal menu che compare in alto a destra (qualora quest'opzione non fosse già disponibile all'interno del nostro account, possiamo attivarla all'interno della sezione "Labs" del menu Impostazioni). Quando ci viene richiesto, consentiamo a mail.google.com di usare Gears: a questo punto partirà uno strumento di sincronizzazione automatica, pronto a salvare su disco tutti i messaggi della nostra casella di posta.

:: Accediamo al database

Quando la sincronizzazione è completa ed entriamo in modalità di connessione instabile possiamo aprire un qualsiasi messaggio senza essere collegati a Internet, possiamo effettuare delle ricerche all'interno della mailbox oppure consultare l'elenco dei nostri contatti. Ciò significa che tutti questi dati sono salvati in locale e quindi accessibili anche fuori dal browser: l'unico problema da risolvere, quindi, è trovarli e capire in che formato sono memorizzati. Per fortuna entrambe le domande hanno una rapida risposta: all'indirizzo http://gears.google.com/support/bin/answer.py?answer=79850 troviamo la posizione in cui vengono salvati i dati offline, a seconda del sistema operativo e del browser utilizzato; aprendo la directory specificata vi sono diverse directory contenenti tutti gli allegati scaricati, insieme ad alcuni file, il cui nome termina con il suffisso

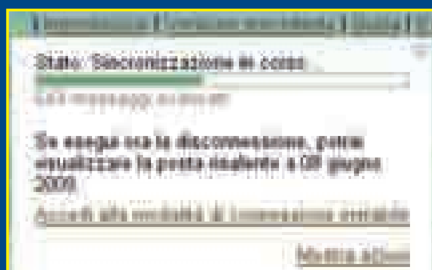


L'opzione "Offline" è solo una delle numerose funzioni sperimentali di Gmail Labs.

#database, che costituiscono la base di dati dei nostri messaggi; visualizzando uno di questi file con un editor esadecimale scopriamo che i database in questione seguono il formato SQLite. SQLite è un DBMS agile e compatto, in grado di salvare un intero database in un singolo file. Grazie a questa sua caratteristica viene usato da diverse applicazioni per memorizzare impostazioni e archivi di ogni sorta (ad esempio, Firefox lo utilizza per gestire cronologia e segnalibri). I database SQLite possono essere aperti con un apposito programma da linea di comando, che può essere scaricato dal sito http://sqlite.org/ (file binari sono disponibili per windows, linux e mac). Per accedere alla nostra casella di posta dobbiamo aprire il database più grande (lanciando il comando sqlite3 indirizzo@gmail.com-GoogleMail#database). Al prompt di SQLite possiamo inserire diversi comandi: ad esempio, .tables mostra l'elenco delle tabelle all'interno del database; .schema <tabella> mostra le colonne presenti all'interno di una tabella e il loro tipo; .dump <tabella> esegue un dump della tabella in SQL; .help mostra l'elenco completo dei comandi di gestione del database. A questi si aggiungono le istruzioni SQL necessarie per leggere il contenuto delle tabelle: possiamo trovare un tutorial dettagliato su questo argomento semplicemente cercando "SQLite tutorial" online, oppure iniziare dalle query di esempio mostrate nel box.

DISCHI PIENI

no dei vantaggi principali di avere Gmail è il fatto di non essere vincolati dai limiti di spazio su disco. Scaricare la posta offline, però, annulla questo vantaggio! Se desideriamo accorciare i tempi di sincronizzazione o se il nostro disco è troppo pieno per contenere tutta la nostra mailbox, nella sezione "Offline" del menu Impostazioni di Gmail possiamo specificare una dimensione massima per gli allegati, oppure scegliere di non scaricarli del tutto.



Il tool di sincronizzazione tiene aggiornata la nostra casella di posta offline.

:: Automatizziamo il tutto

Il vantaggio principale di avere i propri dati salvati in un database è che essi sono accessibili in modo semplice e rapido, utilizzando uno standard (SQL) che è indipendentemente dalla particolare applicazione che li deve utilizzare. Ad esempio possiamo estrarre i dati da linea di comando per poi passarli automaticamente ad altri programmi: per fare questo è sufficiente specificare la query SQL come parametro di sqlite3. Ad esempio, se vogliamo scrivere una mail a tutti quelli con cui abbiamo parlato di un argomento specifico nelle nostre mail passate, possiamo scrivere: thunderbird -compose to="`sqlite3 indirizzo@gmail.com-GoogleMail#database "select distinct c4FromAddress from MessagesFT_Content where c1Body like '%argomento%' "`". È anche possibile accedere al database tramite uno script perl in grado di eseguire operazioni più avanzate: due script di esempio (uno per la ricerca all'interno dei messaggi e uno per l'esportazione dei contatti) sono disponibili online.

LEGGERE LE TABELLE

Per leggere il contenuto di una tabella è necessario eseguire il comando SQL select, specificando i campi desiderati ed eventuali filtri sui dati e terminandolo con un punto e virgola. Ad esempio:

- **select * from Contacts**: mostra l'elenco completo dei contatti;
- **select PrimaryEmail from Contacts where name like '%marco%'**: mostra il solo indirizzo email degli amici chiamati Marco
- **select messagecount, PrimaryEmail from Contacts order by messagecount desc**: mostra l'elenco delle mail ordinato in base al numero di messaggi inviati a ogni indirizzo
- **select c4FromAddress, c0Subject from MessagesFT_Content where c1Body like '%stringa%'**: mostra mittenti e oggetti dei messaggi contenenti "stringa" al loro interno.

Se, poi, vogliamo visualizzare i dati con un'interfaccia un po' più amichevole del semplice terminale, possiamo scaricare l'estensione di Firefox SQLite Manager, reperibile all'indirizzo https://addons.mozilla.org/it/firefox/addon/5817

:: Conclusioni

L'utilizzo di standard come SQL e formati aperti e diffusi come SQLite è certamente una scelta vincente per i produttori di software che, all'atto pratico, possono costruire le proprie applicazioni su una base tecnologica ormai consolidata, basata su formati standard e ben conosciuti. La scelta, però, risulta vincente anche per gli utenti più smaliziati: basta qualche analisi per riconoscere il formato utilizzato e un po' di ragionamento per accedere ai dati come meglio crediamo, senza bisogno di dipendere da un particolare software oppure da qualche servizio online. A questo punto non ci resta che cercare nel nostro disco altri file con estensione .sqlite per vedere cosa nascondono...

mShell

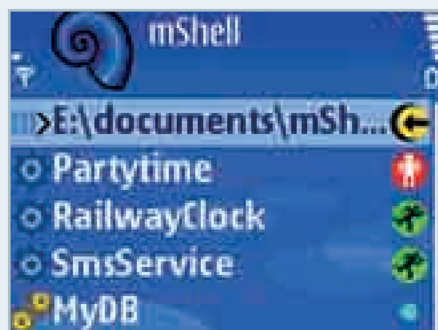
Come rendere il proprio smartphone ancora più smart!

Sembravano ormai lontani i tempi del BASIC, ma in informatica non si butta mai via nulla e non è raro che si possano recuperare vecchi concetti rimasti validi anche con le tecnologie più avanzate. È il caso di mShell (www.m-shell.net), un prodotto dalla Airbit di Zurigo che rifacendosi proprio alla semplicità del BASIC ha creato una piattaforma di sviluppo per smartphone con Symbian che utilizza un suo linguaggio di scripting e permette di scrivere con estrema facilità programmi per i cellulari.

È scontato che si possa accedere alle caratteristiche tipiche del telefonino, come gestire automaticamente gli sms, sfruttare la fotocamera da remoto, gestire applicazioni del cellulare collegandosi via bluetooth dal proprio PC e molto altro (nel box un esempio di script).

:: Caratteristiche di mShell

Sono supportate tutte le versioni di Symbian Serie 60 (dalla 1a alla 3a), UIQ2 e UIQ3 e va quindi installato il pacchetto sis opportuno per il proprio telefono.



L'interfaccia di mShell è semplicissima: vengono visualizzati tutti gli script disponibili e basta cliccarci sopra per lanciarne uno.

Una volta installato e lanciato, mShell chiede se vogliamo registrarci alla community tramite l'invio di un sms (verso la Svizzera), ma possiamo rimandare l'operazione se e quando ne avremo voglia. Per programmi complessi va sicuramente realizzato uno script da lanciare da mShell, tuttavia è supportata anche la modalità interattiva che accetta direttamente i comandi in linea: se ad esempio vogliamo svolgere dei calcoli complessi, possiamo sfruttare mShell come una calcolatrice scientifica evoluta, creando anche funzioni molto complesse. Molto interessante la disponibilità di un debugger integrato: se nel nostro script inseriamo il comando **debug.open**, verrà lanciato il modulo di debug insieme allo script. Nel codice andremo a inserire, nei punti da analizzare, **debug.vlocal(..)** per visualizzare lo stato di alcune variabili, ad esempio inclusi gli array. L'esecuzione verrà interrotta presentando i valori

IL PRIMO PASSO

```
use sms
r="La rivista per veri hacker!";
while true do
  print "Resto in attesa...";
  n=sms.receive(); m=sms.get(n);
  t=lower(trim(m["text"]));
  if t="hj" then
    sms.send(m["sender"], r);
    print "Ho risposto a",m["sender"]
  end
end
```

Un semplice script che resta in attesa di ricevere un sms con scritto "hj". Una volta ricevuto risponde via sms al mittente!

richiesti e per riprenderla si può lanciare il comando **debug.go** e così via (sono presenti diversi tutorial in inglese che spiegano passo passo come sfruttare il debugger).

:: gestione degli script

Nel caso si siano realizzati molti script, in mShell è disponibile la ricerca interattiva (come si fa per cercare un contatto nella rubrica). Dal momento che gli script stessi sono semplici file con estensione .m, possono essere spediti al telefonino da un altro terminale anche via mms o caricati da PC tramite il software che siamo abituati ad usare per l'upload di file. Una volta ricevuto



Ecco un esempio di programmazione interattiva per recuperare una pagina HTML in presenza di una connessione a Internet.

in qualche modo il file, basterà lanciare lo script **inbox2m** che eseguirà una scansione di Inbox alla ricerca dei file con estensioni riconosciute (sono supportati anche gli zip per cui è possibile inglobare più programmi insieme); al termine della scansione presenterà una finestra dove potremo scegliere quali file aggiungere all'indice degli script di mShell.

:: Creiamo il nostro pacchetto sis

Oltre alla modalità a interpretazione, possiamo anche compilare i nostri script e eventuali sottoscript, in un unico eseguibile che sarà sensibilmente più rapido. Il file compilato avrà estensione .mex e potremo sfruttarlo in seguito per creare un pacchetto auto-installante. Per avviare la compilazione dobbiamo lanciare lo script SmsService e poi scegliere Process -> Compile. Una finestra ci chiederà come vogliamo chiamare l'eseguibile e dopo la compilazione avremo l'eseguibile già inserito nella lista dei programmi avviabili da mShell. Per trasformare poi il nostro eseguibile in un pacchetto auto-installante, dobbiamo solo effettuare l'upload del file all'indirizzo www.m-shell.net/Makemsis.aspx e indicare per quale piattaforma vogliamo che sia pronto all'installazione. Clicchiamo su "Create SIS" e in "Your Files" avremo il pacchetto sis risultante.

:: Applicazioni

Le possibilità offerte da una piattaforma software sono infinite, soprattutto visto il potenziale offerto da un pacchetto che, pur se creato commercialmente, viene distribuito gratuitamente. Nel forum presente nel sito ufficiale è possibile accedere alla Wish list (lista dei desideri) delle caratteristiche che altri utenti di mShell vorrebbero venissero introdotte, ma già qualcuno sta andando avanti con gli strumenti a disposizione e ha creato un client MySQL (vedi http://www.m-shell.net/forum.aspx?g=posts&t=405).

Per chi vuole un prodotto già maturo è invece possibile acquistare per circa 24 euro mVNC, un porting del popolare software di controllo remoto realizzato



Anche SmsService può essere compilato per farlo diventare autonomo.

dal team di mShell, che permette di visualizzare su PC il "desktop" del telefonino e pilotarlo come si farebbe dal proprio tastierino o schermo touch. E dato che il controllo è davvero completo, si può accedere a tutto l'hardware a disposizione inclusa la fotocamera! Non ultimo per importanza, viene rilasciato anche il kit per sviluppatori di dll che vogliano estendere le capacità di mShell e gestire quindi nuove caratteristiche. In questo caso le librerie andranno scritte in C/C++ ma viene fornita ampia documentazione sui passi da seguire e sulle API già sviluppate. Con mShell ci si può davvero divertire a trovare nuovi utilizzi per il proprio smartphone.

Massimiliano Brasile

UNA QUERY MYSQL

```
use MySQL;

sql = MySQL.connect("192.168.0.1
",'test','test');
if isstr(sql) then print "Error:
"+sql; proc.stop();end;
MySQL.selectdb(sql,'test')
result = MySQL.query(sql,'select *
from test');
if isstr(result) then print "Error:
"+sql; proc.stop();end;
//print the arrays...
MySQL.disconnect(sql);
```

Codice dimostrativo per creare una query a un database MySQL da mShell.